José M. Muñoz

Introducción a la teoría de conjuntos

CUARTA EDICIÓN

Facultad de Ciencias

UNIVERSIDAD NACIONAL DE COLOMBIA

Departamento de Matemáticas

Introducción a la teoría de conjuntos

CUARTA EDICIÓN

© José M. Muñoz Q.
Facultad de Ciencias
Universidad Nacional de Colombia

Cuarta edición, 2002

Diseño de carátula: Clara I. Bermúdez S.

ISBN: 958-701-168-6

Impresión:
Panamericana, Formas e Impresos S.A.
Calle 65 95-28 teléfono 430 2110
Bogotá, D.C.
COLOMBIA

A Zinnia Nadine, quien me acompaño y alegró durante la redacción de este texto.

Prólogo a la segunda edición

Desde hace algunos años tenía el propósito de redactar unas notas sobre *teoría de conjuntos*, pero mis múltiples ocupaciones me habían impedido hacerlo. Dispuse finalmente del tiempo necesario para tal fin gracias a los dos períodos académicos sin carga docente específica que me concedió la Universidad Nacional de Colombia para dedicarlos a la realización de mi viejo proyecto.

El presente texto ha sido el fruto de este año sabático (Agosto 1978-Julio 1979) y de mis experiencias anteriores como profesor de fundamentos o de teoría de conjuntos para las carreras de matemático y licenciatura en matemáticas.

Aunque al escribirlo siempre tuve en mente a los estudiantes de dichas carreras, también pensé en los profesores de secundaria en ejercicio, de quienes los programas actuales presuponen una preparación que en muchos casos nunca les ha sido dada; de ahí que dediqué una buena parte del libro a construir en detalle los sistemas numéricos.

Atendí siempre en la presentación tanto al rigor como al aspecto pedagógico; la introducción de casi todo concepto o resultado importante está precedida de una motivación, ya sea para interesar al lector en el tema, para hacerle ver la necesidad de efectuar determinada demostración o para ponerle de presente las futuras dificultades.

Para plantear algunos problemas interesantes, he supuesto de los lectores conocimientos ajenos a la teoría expuesta; cuando sobrepasan cierto nivel, los ejercicios llevan a su izquierda +; los ejercicios menos fáciles van precedidos del símbolo * y/o van sucedidos de una ayuda.

A nivel institucional, deseo expresar mi gratitud a la Universidad Nacional de Colombia por haberme dispensado el tiempo necesario para la elaboración de estas notas.

A nivel personal, quiero agradecer a mi esposa y a mis hijos su comprensión, el apoyo que me brindaron y el tiempo de merecido descanso que sacrificaron y me cedieron para dedicarlo a la redacción de este libro. También deseo expresar mis agradecimientos a los profesores de la Universidad Nacional José Darío Sánchez H. y Clara Helena Sánchez B., quienes usaron en sus cursos la edición de prueba e hicieron sugerencias valiosas para mejorar el texto.

José M. Muñoz Quevedo
Profesor Emérito
Departamento de Matemáticas y Estadística
Universidad Nacional de Colombia

Bogotá D. E. 1983.

Prólogo a la cuarta edición

Me llena de satisfacción poner a disposición de profesores y estudiantes esta cuarta edición de la obra que más aprecio entre las pocas que he escrito. Procuré mejorarla al máximo dentro de mis posibilidades. Sus diferencias principales con respecto a la segunda edición son las siguientes:

Se incluyó una sección sobre las relaciones entre los cuantificadores y los conectivos lógicos.

Se amplió la sección donde se bosqueja la construcción de un lenguaje lógico de primer orden.

Se dieron nuevas formas de efectuar definiciones por recurrencia aplicables en diferentes ramas de la matemática.

Se introdujo tempranamente el axioma de eleccción con el fin de usarlo en la obtención de enumeraciones de conjuntos mediante funciones sobreyectivas.

Se introdujo el axioma de fundamentación y se derivaron sus principales consecuencias en lo que respecta a la estructura interna de los conjuntos.

Se agregó una prueba directa, sencilla y elegante del axioma de completez de $\mathbb{R}$.

Se adicionó una nueva demostración del Teorema de Cantor-Bernstein, usando el "Lema del Punto Fijo", la cual fue elaborada por el profesor Luis Rafael Jiménez, a quien agradezco su gentileza.

Se introdujo tempranamente el axioma de sustitución, se destacó su importancia y se probó que éste implica tanto al axioma de separación como al axioma del conjunto con dos elementos.

Se agregó un capítulo completo sobre los números ordinales, tratándolos en la forma más sencilla posible como extensiones de los números naturales. poniendo de presente el papel que juegan como clasificadores de los conjuntos bien ordenados.

Se mejoraron ostensiblemente tanto los dibujos como la presentación general del texto, el cual se procesó en LaTeX.

Hoy, más de veinte años después de la primera edición, surge la pregunta: ¿es un texto aún vigente? Los temas tratados corresponden a los que podrían llamarse tópicos básicos eternos, de conocimiento imprescindible para el futuro matemático o para el licenciado en Matemáticas. Si bien es cierto que en el texto no se incluye ningún resultado reciente en teoría de conjuntos, debido a que su comprensión requiere una madurez y un nivel de conocimientos mayores a los que poseen los estudiantes de cuarto semestre universitario, se recomienda a los docentes habilidosos subsanar esta carencia, haciendo la introducción, al menos a un tema contemporáneo, como las técnicas de forzamiento de Cohen, el cual, aun cuando de nivel mayor que el del presente texto, se ha transformado en un tópico eterno muy fructífero en teoría de modelos.

Una vez más agradezco a la Universidad Nacional su interés y apoyo para que esta nueva edición se hiciera realidad, en especial al Coordinador de publicaciones del Departamento de Matemáticas y Estadística, profesor Gustavo Rubiano por su interés en que esta nueva edición saliera con una gran calidad editorial. Quiero agradecer a los hoy matemáticos Leonardo Prieto y Franqui Cárdenas por el levantamiento del texto de la tercera edición en TeX, a mi hermana, la profesora Myriam Muñoz de Ozak y a los estudiantes William Llanos y Maira Saldaña por la elaboración de los dibujos y por su trabajo complementario en el tratamiento, corrección y transportación del texto matemático de TeX al procesador LaTeX, y finalmente al profesor Yu Takeuchi por sus útiles sugerencias para el mejoramiento conceptual del presente libro, el cual espero siga siendo de utilidad para estudiantes y profesores.

Jose M. Muñoz Quevedo
Profesor Honorario.
Departamento de Matematicas.
Universidad Nacional de Colombia.

Bogotá D.C, 2002.

Índice General

1 DESARROLLO INTUITIVO **1**
- 1.1 PROPOSICIONES Y CONECTIVOS 1
- 1.2 CONJUNTOS 12
- 1.3 OPERACIONES ENTRE CONJUNTOS 18
- 1.4 CONECTIVOS Y CUANTIFICADORES 27
- 1.5 COLECCIONES DE CONJUNTOS 31
- 1.6 ALGUNAS PARADOJAS 36
- 1.7 CONSTRUCCIÓN DE UN LENGUAJE 41

2 DESARROLLO AXIOMÁTICO **49**
- 2.1 PRIMEROS AXIOMAS 49
- 2.2 REUNIONES Y CONJUNTOS DE PARTES 59

3 FUNCIONES Y RELACIONES **63**
- 3.1 EL PRODUCTO CARTESIANO 63
- 3.2 RELACIONES 72
- 3.3 FUNCIONES 78
- 3.4 COMPOSICIÓN DE FUNCIONES 91
- 3.5 PROPIEDADES DE LAS RELACIONES 102
- 3.6 RELACIONES DE EQUIVALENCIA 109
- 3.7 RELACIONES DE ORDEN 118

4 LOS NÚMEROS NATURALES **129**
- 4.1 CONSTRUCCIÓN DE LOS NATURALES 130
- 4.2 EL ORDEN DE LOS NATURALES 141
- 4.3 INDUCCIÓN MATEMÁTICA 148
- 4.4 OPERACIONES ENTRE NATURALES. 157

5 CONSTRUCCIÓN DE LOS SISTEMAS NUMÉRICOS 169
5.1 LOS NÚMEROS ENTEROS 169
5.2 LOS NÚMEROS RACIONALES. 177
5.3 LOS NÚMEROS REALES 183
5.4 LOS NÚMEROS COMPLEJOS. 204

6 CONJUNTOS INFINITOS Y CARDINALES 209
6.1 CONJUNTOS INFINITOS 209
6.2 FORMAS DEL AXIOMA DE ELECCIÓN 219
6.3 CONJUNTOS CONTABLES 227
6.4 CONJUNTOS NO CONTABLES 237
6.5 NÚMEROS CARDINALES 244

7 ELECCIÓN, CARDINALIDAD Y REGULARIDAD 255
7.1 ORDEN Y ELECCIÓN 255
7.2 ELECCIÓN Y CARDINALIDAD 263
7.3 EL AXIOMA DE FUNDAMENTACIÓN 268
7.4 EL AXIOMA DE REEMPLAZO 274

8 NUMEROS ORDINALES 277
8.1 ÓRDENES SEMEJANTES 277
8.2 NÚMEROS ORDINALES 283
8.3 CONJUNTOS DE ORDINALES 288

Capítulo 1

DESARROLLO INTUITIVO

1.1 PROPOSICIONES Y CONECTIVOS

El que los conceptos de conjunto, elemento y pertenencia sean los más intuitivos de la Matemática, no es casual; en realidad el conocimiento, en cualquier rama de la ciencia puede darse mediante relaciones conjuntistas o al menos descansa en un lenguaje que la persona ha adquirido a través de una serie de vivencias de tipo conjuntista.

Para mejorar nuestra intuición en lo que a los conjuntos se refiere y para corregirle posibles desviaciones, lo mismo que para que sirva de base a la teoría axiomática posterior, dedicamos esta primera parte a desarrollar en forma puramente intuitiva la teoría de los conjuntos.

El primer concepto que necesitamos para llevar a cabo nuestro estudio es el de "*proposición*". Es una palabra tomada del lenguaje corriente en el cual significa más o menos "expresión con sentido completo". Nosotros seremos un poco más exigentes y usaremos la palabra *proposición* tan sólo para designar *aquellas expresiones de las cuales tiene sentido afirmar que son verdaderas o falsas.*

Por ejemplo,

"$1 + 1 = 2$"

"Bogotá es la capital de Colombia"
"Sir Wiston Churchill fue presidente de Francia"
"Existen triángulos isósceles que no son equiláteros"
"Todos los hombres son mortales"

"En Colombia existen 40'487.521 habitantes actualmente", son proposiciones en el sentido matemático (que será en el único sentido con el cual usaremos esta palabra en adelante).

No son proposiciones ("aun cuando tienen sentido completo") las expresiones siguientes:
"Buenos días "
"¿Cómo está Ud.?"
"x es blanco"
"Señor, ayúdeme a empujar este automóvil, por favor".

La razón se halla en que carece de sentido afirmar que ellas sean verdaderas o falsas.

En esta sección *no* vamos a interesarnos en el significado de las proposiciones; únicamente las analizaremos desde el punto de vista de su veracidad: ***nos importará saber si una proposición es verdadera o falsa*** y tan sólo estudiaremos proposiciones que sean verdaderas o falsas.

Es costumbre emplear las letras p, q, r, s, etc. como símbolos para designar proposiciones.

Observemos algunas proposiciones de la vida corriente:

(a) "Está bien, dijo José Arcadio Buendía. Nos iremos de este pueblo lo más lejos que podamos y no regresaremos jamás". (G. García Márquez, *Cien años de Soledad).*

(a′) Pagaré la comida y la bebida.

(b) Llevaré a mi novia flores o le llevaré dulces.

(c) "Si te gusta escuchar, aprenderás. Si inclinas tu oído, serás sabio" (Salomón, *Los Proverbios*).

(c′) Si la gasolina sube de precio, entonces también aumentará el precio de todos los artículos que se transportan.

(d) Se producirá un cambio sustancial en nuestro país si y solamente si, las clases media y baja comienzan a actuar masivamente en defensa de sus intereses.

(e) "En Santa Fe de Bogotá son las cinco de la tarde del 25 de septiembre de 1828. Para los conspiradores el ambiente es tenso; en unas horas más Bolívar estará vivo o muerto; todo depende de las circunstancias".

(e′) "Ser o no ser: he ahí el problema" (Shakespeare,*Hamlet*).

(f) "Si prescindimos del contenido material de la circulación de mercancías y nos limitamos a analizar las formas económicas que este proceso engendra, veremos que el resultado final es el dinero".(Marx, *El Capital*).

Notamos que son proposiciones con cierta complejidad, llamadas *compuestas* debido a que constan de dos o más proposiciones unidas o concatenadas mediante partículas del lenguaje llamadas *conjunciones* (sirven para "juntar" proposiciones). Así encontramos en (a) y en (a′) la conjunción "y" (integrando dos proposiciones en otra mayor), en (b) la conjunción "o", en (c) tenemos "si ... entonces ... ", en (d) hallamos "... si y sólo si ... ", en (e) nuevamente la "o" usada en un sentido diferente y (f) posee una forma un poco más compleja "si ... y ... , entonces ... ".

Aun cuando en un idioma existen otras conjunciones (ni ... ni ... , ... pero ... , ... mas no ... , etc.), el papel que ellas desempeñan puede llevarse a cabo con las cinco nombradas anteriormente y la partícula "no ", usada para negar proposiciones.

Si p es una proposición, es costumbre simbolizar $\neg p$ a su negación (léase "no p" o la "negación de p"). Por ejemplo, si p es la proposición "$1+5=7$", $\neg p$ será "$1+5\neq 7$"; si q designa "Bogotá es la capital de Colombia ",$\neg q$ será "Bogotá no es la capital de Colombia".

Se nota que si una proposición es verdadera, su negación es falsa y recíprocamente, si una proposición es falsa, su negación es verdadera.

Usando las letras V y F para simbolizar "Verdadero" y "Falso" respectivamente, la observación anterior se puede resumir en una tabla (llamada tabla de verdad) como la siguiente:

p	$\neg p$
V	F
F	V

Bajo "p" aparecen V y luego F para indicar que p puede ser verdadera o falsa; la primera línea horizontal de valores de verdad significa que si p es verdadera, $\neg p$ es falsa y la segunda, que cuando p es falsa, $\neg p$ es verdadera.

Analicemos ahora la proposición (a): Es una proposición compuesta que se ha obtenido uniendo otras dos mediante la conjunción "y". Si designamos con "p" a la proposición "nos iremos de este pueblo lo más lejos que podamos" y con "q" a la proposición "no regresaremos jamás", entonces (a) se puede representar por p y q. Es costumbre en matemáticas usar el signo "$\wedge$" para la conjunción "y", evitando confusiones posteriores con la

letra "y", usada como variable (en las ecuaciones, por ejemplo). Siguiendo la costumbre, la proposición (a) se simbolizará "$p \wedge q$".

Del lenguaje común se deduce que una proposición que posee la forma $p \wedge q$ es verdadera tan sólo cuando las proposiciones componentes p, q son simultáneamente verdaderas. Por ejemplo si no se van lejos del pueblo, la proposición (a) es falsa; lo mismo si se van y regresan. La proposición (a′) hace ver que si tanto p como q son falsas, "$p \wedge q$" también es falsa.

Podemos utilizar una tabla de verdad para sintetizar el párrafo anterior: Cada línea horizontal corresponde a uno de los casos anotados anteriormente; así la tercera línea significa que cuando p es falso y q es verdadero, $p \wedge q$ es falso.

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Nótese que hay cuatro líneas horizontales ya que hay cuatro casos posibles, en cuanto a la veracidad de p y q se refiere; estos casos se pueden hallar escribiendo en la columna bajo p dos veces consecutivas V y luego dos veces consecutivas F, y en la columna bajo q se escriben alternadamente V, F, V, F. En esta forma lo haremos en adelante para construir las tablas de verdad de las otras conjunciones.

Supongamos que Juan dice "Llevaré a mi novia flores o dulces ". Si tan sólo le lleva flores, Juan ha dicho la verdad; si solamente le lleva dulces, también ha dicho la verdad; si le lleva flores y dulces, Juan queda espléndidamente es decir, una vez más ha dicho la verdad; pero si no le llevara flores y tampoco le llevara dulces, Juan sería un mentiroso, habría dicho una falsedad.

Este ejemplo pone de presente que en este caso la conjunción "o" se ha usado para indicar que una proposición de la forma "p o q" es falsa únicamente cuando tanto p como q son falsas. En Matemáticas se prefiere escribir "$p \vee q$" para precisar que la conjunción "o" se está usando en el sentido descrito; su tabla de verdad es la primera de las dos que siguen.

Las proposiciones (e) y (e′) ponen de presente otro uso frecuente de la partícula "o"; las dos proposiciones ligadas por ellas son mutuamente excluyentes: "vivo o muerto", "ser o no ser". Si es verdad que esté vivo, es falso que esté muerto, si es falso que esté vivo, es verdad que esté muerto: no se puede estar vivo y muerto simultáneamente. Tampoco se puede no estar vivo y no estar muerto a la vez. Para distinguir este nuevo uso de "o"

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

p	q	$p \veebar q$
V	V	F
V	F	V
F	V	V
F	F	F

del anterior, introducimos el signo "$\veebar$" y lo llamaremos el "o exclusivo". Hemos resumido lo dicho en la tabla anterior de la derecha.

Es corriente referirse a las tres proposiciones compuestas anteriores así:

$p \wedge q$: la conjunción de p, q

$p \vee q$: la disyunción inclusiva de p, q

$p \veebar q$: la disyunción exclusiva de p, q.

Pasemos a analizar el uso de "si p, entonces q" que se simboliza "$p \rightarrow q$" y también se lee "p implica q". Nadie pone en duda la verdad de una proposición como si "Colombia posee más de un millón de Km^2 de superficie, entonces la superficie de Colombia es mayor que la de Suiza", en la cual tanto la primera componente como la segunda son verdaderas.

Evidentemente "Si Colombia posee 1'138.338 Km^2 y Brasil 8'511.965 de superficie, entonces Colombia posee más superficie que Brasil" es una proposición falsa; aquí la primera proposición componente es verdadera y la segunda es falsa.

De otra parte, las siguientes son consideradas frases *correctas* (léase *proposiciones verdaderas*).

(i) Si en Colombia hay cien millones de habitantes, entonces en Colombia hay más habitantes que en el Ecuador.

(ii) Si en Colombia hay aproximadamente cien millones de hombres casados, entonces en Colombia hay aproximadamente cien millones de mujeres casadas.

Nótese que en (i) la primera proposición componente es falsa y la segunda es verdadera, en tanto que en (ii) las dos proposiciones componentes son falsas.

Motivados por razones como las aducidas mediante los ejemplos anteriores y analizando su posterior buen desempeño, los matemáticos han

tomado como tabla de verdad para la implicación la siguiente:

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

Algunas veces "$p \to q$" se lee "p es una condición suficiente para q" o "q es una condición necesaria para p". Proposiciones como la (d) del comienzo, las cuales poseen la forma "p si y sólo si q", se acostumbran simbolizar "$p \leftrightarrow q$"; se lee "p es una condición necesaria y suficiente para q" o más frecuentemente "p es equivalente a q".

Entendiéndose que la equivalencia se considera respecto de la veracidad de las proposiciones componentes, "p" y "q" serán equivalentes tan solo cuando las dos sean simultáneamente verdaderas o simultáneamente falsas; su tabla de verdad es la siguiente.

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

En lo sucesivo, consideramos las tablas de verdad anteriormente dadas como las definiciones de los símbolos $\neg, \wedge, \vee, \underline{\vee}, \to, \leftrightarrow$, a los cuales nos referiremos como los *conectivos proposicionales.*

Las proposiciones compuestas que hemos estudiado hasta este momento contienen tan solo un conectivo proposicional, pero muchas veces necesitamos emplear proposiciones más complejas en las cuales aparezcan dos o más conectivos proposicionales (un número finito de ellos). Por ejemplo, la proposición (f) del comienzo tiene la forma $(p \wedge q) \to r$; otras pueden ser $p \vee (\neg p)$, $(p \wedge (\neg p)) \to q$, $\neg((p_1 \wedge p_2) \vee (p_3 \leftrightarrow ((p \wedge q) \vee (p \wedge r))))$, etc. Nótese que los paréntesis son un gran auxiliar para dar un significado preciso a las expresiones.

La intuición nos dice generalmente cómo mezclar proposiciones y conectivos; sin embargo para evitar la pérdida de tiempo tratando de hallar el sentido a expresiones como $(p\neg) \wedge q$, $(\to q \vee \wedge sy) \to (\neg)p \wedge (\underline{\vee}s) \leftrightarrow$, daremos a continuación las normas para obtener únicamente expresiones con "sentido", a las cuales llamaremos *fórmulas bien formadas* (abreviación: f.b.f.), es decir, las reglas sintácticas del llamado *cálculo proposicional.*

En adelante, además de p, q, r, usaremos $p_1, p_2, p_3, \ldots$ como símbolos para designar proposiciones y nos referiremos a ellos como a los *símbolos proposicionales.* Teniendo tantos símbolos proposicionales como números naturales, disponemos de una buena cantidad de ellos, suficiente para representar cualquier proposición que tengamos en la memoria; seguramente una persona no alcanza en toda su vida a fijar en su mente más proposiciones que números naturales. Así, podemos considerar que cada símbolo representa una única proposición simple.

Las reglas que gobiernan las fórmulas bien formadas ("expresiones con sentido") son:

(1) Los símbolos proposicionales son fórmulas bien formadas.

(2) Si α es una f.b.f., entonces su negación $(\neg\alpha)$ es una f.b.f.

(3) Si α y β son f.b.f., entonces también lo son
$(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \underline{\vee} \beta)$, $(\alpha \to \beta)$, y $(\alpha \leftrightarrow \beta)$.

(4) Una expresión es una fórmula bien formada si y sólo si el que lo sea se sigue de aplicar las reglas (1). (2), (3) finitas veces.

La regla (4) significa que las únicas f.b.f. son las que se pueden construir combinando (1), (2), (3) un número finito de veces. En consecuencia, supongamos que nos dan una expresión como

$$((\neg(p_1 \to p_2)) \vee (p_3 \leftrightarrow (\neg p_4)))$$

para averiguar si es una f.b.f. o no. De acuerdo con (4), debemos tratar de construirla usando las reglas (1), (2) y (3);

(i) p_1, p_2, p_3, p_4 son f.b.f. de acuerdo a (1).

(ii) $(p_1 \to p_2)$ es f.b.f. según (3).

(iii) $(\neg(p_1 \to p_2))$ es f.b.f. según (2).

(iv) $(\neg p_4)$ es f.b.f. por (2).

(v) $(p_3 \leftrightarrow \neg(p_4))$ es f.b.f. aplicando la regla (3) ya que p_3 y $(\neg p)$ lo son.

(vi) Aplicando la regla (3) a (iii) y (v) se obtiene que
$((\neg(p_1 \to p_2)) \vee (p_3 \leftrightarrow (\neg p_4)))$ es f.b.f.

Una expresión como) $\rightarrow (\neg p) \wedge (\underline{\vee} s) \leftrightarrow$ no es una fórmula bien formada ya que s es f.b.f. pero "$\underline{\vee} s$ " no lo es y el proceso de formación no puede continuarse.

Nota. Para simplificar la escritura, en adelante, eliminaremos la mayor cantidad posible de paréntesis, siempre y cuando no se produzcan confusiones. Por ejemplo, no volveremos a escribir el paréntesis inicial ni el final; convendremos en que el símbolo de negación actúa sobre la f.b.f. más corta que está a su derecha (Así $\neg p \vee q$ es $((\neg p) \vee q)$; si queremos que $\neg$ actúe sobre $p \vee q$, colocamos el paréntesis: $\neg(p \vee q)$). Cuando hay presentes varios conectivos, suponemos que primero actúa $\neg$, después actúan $\vee, \underline{\vee}, \wedge$ y luego sí $\rightarrow, \leftrightarrow$. Por ejemplo, $p \wedge q \rightarrow p \vee q$ es $((p \wedge q) \rightarrow (p \vee q))$. En $p \vee (p \wedge r)$, $p \rightarrow (q \leftrightarrow r)$ los paréntesis son indispensables, no pueden suprimirse.

Como una f.b.f. se ha obtenido a partir de finitos símbolos proposicionales por aplicación de (1), (2) y (3) finitas veces, siempre es posible construir su tabla: se dan a los símbolos proposicionales que aparecen en la f.b.f. los valores V, F combinados adecuadamente para obtener todos los casos posibles y luego se van construyendo paso a paso las tablas de verdad de las f.b.f. que se han ido formando hasta llegar a la f.b.f. dada inicialmente (Nótese que si aparecen n símbolos proposicionales en una f.b.f., su tabla de verdad tendrá 2^n filas, correspondientes a las 2^n formas posibles de combinar V y F).

Unos ejemplos aclararán lo dicho: Construir las tablas de verdad de $p \vee \neg p$, $(p \wedge q) \rightarrow p$, $(p \vee q) \wedge \neg p$, de $\alpha := p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$ y de $(p \vee q) \longrightarrow p$.

Si observamos las tablas de verdad siguientes, vemos que existen fórmulas bien formadas como $p \vee \neg p$, $(p \wedge q) \rightarrow p$, y la que hemos llamado α, tales que en su tabla de verdad únicamente aparece el valor V, sin importar la verdad o falsedad de sus proposiciones componentes; se llaman *tautologías*. Son las f.b.f. más importantes, debido a que corresponden a proposiciones compuestas que intuitivamente son *verdaderas*, independientemente de la veracidad de sus componentes. Podemos hacernos la siguiente pregunta: ¿Dada una f.b.f., existe un procedimiento para averiguar si es una tautología o no?

La respuesta es evidentemente afirmativa: basta construir su tabla de verdad; si en ella sólo aparece V, es tautología; en el caso contrario, no lo es.

p	q	$p \wedge q$	$(p \wedge q) \rightarrow p$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

p	q	$p \vee q$	$(p \vee q) \rightarrow p$
V	V	V	V
V	F	V	V
F	V	V	F
F	F	F	V

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

p	q	$p \vee q$	$\neg p$	$(p \vee q) \wedge (\neg p)$
V	V	V	F	F
V	F	V	F	F
F	V	V	V	V
F	F	F	V	F

p	q	r	$q \vee r$	$p \wedge q$	$p \wedge r$	$p \wedge (p \vee r)$	$(p \wedge q) \vee (p \wedge r)$	α
V	V	V	V	V	V	V	V	V
V	V	F	V	V	F	V	V	V
V	F	V	V	F	V	V	V	V
V	F	F	F	F	F	F	F	V
F	V	V	V	F	F	F	F	V
F	V	F	V	F	F	F	F	V
F	F	V	V	F	F	F	F	V
F	F	F	F	F	F	F	F	V

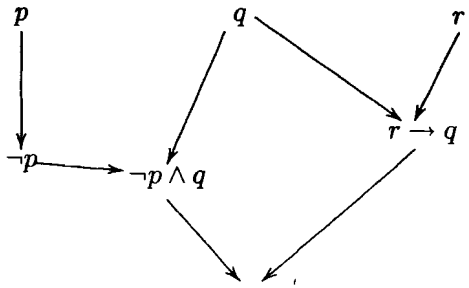
A continuación damos una lista de algunas otras tautologías que usaremos más adelante; la demostración de que efectivamente son tautologías, la dejamos al lector:

1) $(p \vee p) \leftrightarrow p$; $(p \wedge p) \leftrightarrow p$
2) $p \vee q \leftrightarrow q \vee p$
3) $(p \vee q) \vee r \leftrightarrow p \vee (q \vee r)$.
4) $p \wedge (q \underline{\vee} r) \leftrightarrow (p \wedge q) \underline{\vee} (p \wedge r)$
5) $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
6) $(p \wedge q) \wedge r \leftrightarrow p \wedge (q \wedge r)$
7) $(p \wedge q) \wedge p \leftrightarrow p \wedge q$
8) $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$
9) $p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$
10) $(p \rightarrow (q \rightarrow r)) \leftrightarrow (p \wedge q \rightarrow r)$
11) $[p \rightarrow (q \rightarrow r)] \rightarrow [(p \rightarrow q) \rightarrow (p \rightarrow r)]$
12) $\neg(p \leftrightarrow q) \leftrightarrow ((p \wedge \neg q) \vee (\neg p \wedge q))$
13) $\neg(\neg p) \leftrightarrow p$
14) $(p \rightarrow q) \leftrightarrow (\neg p \cdot q)$
15) $(p \underline{\vee} q) \underline{\vee} r \leftrightarrow p \underline{\vee} (q \underline{\vee} r)$
16) $(p \vee q) \vee p \leftrightarrow p \vee q$
17) $p \wedge q \leftrightarrow q \wedge p$
18) $\neg(p \vee q) \leftrightarrow \neg p \wedge \neg q$
19) $\neg(p \rightarrow q) \leftrightarrow p \wedge \neg q$
20) $\neg(p \leftrightarrow \neg p)$
21) $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$
22) $\neg(p \wedge \neg p)$
23) $(p \wedge (p \rightarrow q)) \rightarrow q$
24) $p \rightarrow (q \rightarrow p)$

Ejercicios

1. Demuestre que todas las f.b.f. de 1) a 24) anteriormente listadas son tautologías.

2. Una forma abreviada de escribir la demostración de que una expresión es una f.b.f., es construyendo lo que podríamos llamar su árbol genealógico; partiendo de los símbolos proposicionales, se va formando poco a poco aplicando las reglas (1), (2) y (3) dadas anteriormente; como ejemplo construyamos el de $(\neg p \wedge q) \vee (r \rightarrow q)$:



   Use este procedimiento para decidir cuáles de las siguientes expresiones son f.b.f. y cuales nó:

   (a) $(\neg p \rightarrow \neg q) \rightarrow \neg(p \vee q)$.
   (b) $p \rightarrow \underline{\vee} \neg r \wedge q$.
   (c) $(p_1 \wedge p_2) \wedge p_3 \leftrightarrow (\neg p_4 \vee p_3)$.
   (d) $((p_1 \rightarrow (\neg p_2)) \wedge p_1) \rightarrow \neg p_2$.
   (e) $p \wedge q \vee p \wedge r$.
   (f) $(\neg \vee p) \rightarrow (q \wedge r)$.
   (g) $\neg(p \wedge q) \rightarrow ((\neg p) \wedge (\neg q))$.

3. Use las tablas de verdad para probar que $(p \wedge \neg p) \rightarrow q$ es una tautología.

4. Sean α, β fórmulas bien formadas. Se dice que "α implica tautológicamente a β" si $\alpha \rightarrow \beta$ es una tautología. Se dice "α es tautológicamente equivalente a β" si α implica tautológicamente a β y β implica tautológicamente a α, o lo que es igual si $\alpha \leftrightarrow \beta$ es una tautología. Halle cinco ejemplos de implicación tautológica y cinco de equivalencia tautológica.

5. Una *contradicción* es una f.b.f. compuesta que siempre es falsa, independientemente de la veracidad de las proposiciones componentes. Dé cinco ejemplos de contradicciones, demostrando que lo son mediante tablas de verdad si es del caso.

6. Dadas las proposiciones p : Hace frío y q : Está de noche, y suponiendo que la primera es verdadera en este momento y la segunda falsa, escriba en términos de p, q y los conectivos, las proposiciones siguientes y halle sus valores de verdad:

   (a) No está de noche o no hace frío.
   (b) Hace frío o no está de noche.
   (c) Ni está de noche ni hace frío y
   (d) Está de noche pero no hace frío.

7. Halle la negación de cada una de las proposiciones anteriores dando la respuesta tanto en términos de p, q y los conectivos, como en español correcto.

1.2 CONJUNTOS

Un enjambre de abejas, un ejército, un rebaño de ovejas, son ejemplos de conjuntos.

Siendo, como lo hemos dicho antes, los conceptos de *conjunto, elemento* y *pertenencia* los más intuitivos de la Matemática, los consideraremos como los conceptos primitivos de este estudio, es decir, no trataremos de definirlos sino que iremos simultáneamente trabajando con ellos y precisándolos mediante sus propiedades.

Nuestro sentido común nos dice que podemos determinar un conjunto de dos maneras:
1) Dando una lista de los objetos o elementos que lo forman o
2) Dando la condición o las condiciones que deben cumplir sus elementos; estas condiciones deberán ser lo suficientemente precisas para que dado cualquier objeto, podamos decidir si pertenece o no al conjunto en cuestión.

Cuando se determina un conjunto mediante una lista, es costumbre decir que se está determinando por *extensión* y escribir sus elementos entre dos llaves; por ejemplo,

$$\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}$$

es el conjunto de los números llamados dígitos en tanto que

$$\{3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19\}$$

es el de los números primos mayores que 2 y menores que veinte.

Nótese que con la frase anterior estamos definiendo al mismo conjunto $\{3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19\}$ por medio de las condiciones que cumplen sus elementos: éstos deben ser números naturales (o enteros), primos, mayores que dos y menores que 20. Decimos en este caso que estamos definiendo al conjunto por *comprensión* y lo escribimos así:

$$\{x \mid x \text{ es un número natural primo} \wedge x \text{ es mayor que } 2 \wedge x \text{ es menor que } 20\}.$$

Se puede leer como "El conjunto de los elementos x tales que ..." yendo en el sitio de los puntos suspensivos la condición que determina el conjunto. Si denotamos por $p(x)$ a una condición redactada en términos de x, el conjunto determinado por ella se escribe entonces

$$\{x \mid p(x)\} \qquad \text{o} \qquad \{x : p(x)\}$$

Nota: Usaremos también la palabra *colección* como sinónimo de conjunto.

Por ejemplo, los siguientes cinco conjuntos están definidos por comprensión:
$A = \{x \mid x \text{ es capital de un país suramericano }\}$.
$B = \{x \mid x \text{ es mexicano} \wedge x \text{ mide más de 4 metros de estatura }\}$.
$C = \{x : x \text{ ha sido presidente de Colombia en este siglo }\}$.
$D = \{x : x \text{ es número natural} \wedge (x \text{ es divisor de } 12 \vee x \text{ es divisor de } 20)\}$.
$E = \{x \mid x \text{ es una ciudad} \wedge x \text{ es la capital de Colombia }\}$.

Este último E es precisamente el conjunto { Bogotá} constituído por un solo elemento, razón por la cual se llama *unitario.*

Como no existen en México personas que cumplan la condición de medir más de 4 metros de estatura, el conjunto B no posee elementos: $B = \{\ \}$; se le llama *conjunto vacío* y con frecuencia también se nota $\emptyset$.

Para indicar que "4 es un elemento del conjunto D", escribimos "$4 \in D$" y también lo leeremos "4 pertenece al conjunto D" o "4 está en D ". En vez de $\neg(a \in D)$ escribiremos $a \notin D$. Al símbolo " $\in$" se le acostumbra llamar de *pertenencia.*

Al leer una condición como "x mide más de 1.5 metros de alto", podemos pensar que se está haciendo referencia a personas, jirafas, árboles, camiones, etc. La sola condición no basta; es necesario dar además un conjunto *no vacío* acerca de cuyos elementos nos referimos en la condición; un conjunto tal se llama un *conjunto referencial* o simplemente un referencial (para la condición dada). Por ejemplo, para la condición "$x^3 - x^2 - 9x + 9 = 0$" podríamos tomar como referencial a cualquiera de los conjuntos { 0, 1, 2}, {1, 2, 3, 4, 5}, {-3, -2, -1, 0}, $\mathbb{R}$, etc. pero no nos serviría un conjunto de personas ni un conjunto de ciudades. Debe existir una inter-relación entre referencial y condición: Cada vez que reemplacemos "x" por un elemento del referencial, la condición se debe transformar en una proposición (unas veces verdadera y otras falsa). Así por ejemplo, si tomamos como referencial $S = \{1, 2, 3, 4, 5\}$ y como condición "$x^3 - x^2 - 9x + 9 = 0$", al reemplazar a"x" por 2, 4 y 5 ($2^3 - 2^2 - 9 \cdot 2 + 9 = 0, 4^3 - 4^2 - 9 \cdot 4 + 9 = 0$, etc.) obtenemos proposiciones falsas y al reemplazar "x" por 1 y por 3, obtenemos proposiciones verdaderas:

$$1^3 - 1^2 - 9 \cdot 1 + 9 = 0; \qquad 3^3 - 3^2 - 9 \cdot 3 + 9 = 0.$$

Se dice que 1 y 3 satisfacen (o cumplen) la condición dada y

$$\{1,\ 3\} = \{x \in S | x^3 - x^2 - 9x + 9 = 0\}$$

es decir, $\{1, 3\}$ es le conjunto definido por la condición "$x^3-x^2-9x+9 = 0$", respecto del referencial S.

Si S es el conjunto de todos los americanos y $p(x) : x$ es colombiano, $P = \{x \in S \mid p(x)\}$ es el conjunto de todos los colombianos.

Supongamos dado un conjunto referencial S fijo; si $p(x)$ es una condición sobre (los elementos de) S, al símbolo x que puede reemplazarse por un elemento cualquiera del referencial se le llama una **variable**. A un símbolo que representa un elemento bien determinado del referencial (el mismo durante todo el estudio), se le llama una **constante**.

Por ejemplo, si $S = \mathbb{R}$ y $q(y)$ es "$y^2 - 3y + 2 = 0$", entonces "y" es una variable, en tanto que 2, 0, 3 son constantes.

Un concepto derivado del de conjunto es el de subconjunto: Un conjunto A es un subconjunto de B (se nota $A \subseteq B$) si y solo si *todo* elemento de A es un elemento de B. Por ejemplo $\{1, 2, 3\} \subseteq \{2, 4, 0, 1, 3\}$ y este último a su vez es un subconjunto propio de $\mathbb{R}$ [1].

Sea $S = \mathbb{R}$ y consideremos las siguientes condiciones sobre $\mathbb{R}$:

$$p_1(x) : x^2 - 5x + 6 = 0$$
$$p_2(x) : x^2 + 1 = 0$$
$$p_3(x) : x^2 - 1 = (x - 1)(x + 1).$$

Los subconjuntos del referencial S definidos por $p_1(x)$, $p_2(x)$ y $p_3(x)$, son

$$P_1 = \{2, 3\}, \qquad P_2 = \emptyset \qquad \text{y} \qquad P_3 = \mathbb{R} = S,$$

respectivamente. Es costumbre escribir $(\exists x)(p_1(x))$ para significar que el conjunto determinado por $p_1(x)$ no es vacío. Nótese que $(\exists x)(p_1(x))$ ya es una proposición; por ejemplo $(\exists x)(x^2 + 1 = 0)$ es una proposición falsa. Cuando el conjunto determinado por una condición $q(x)$ es todo el referencial, se escribe $(\forall x)(q(x))$.

Por ejemplo, "$(\forall x)(x^2 - 1 = (x - 1)(x + 1))$" es una proposición verdadera, en tanto que $(\forall x)(p_1(x))$ y $(\forall x)(p_2(x))$ son proposiciones falsas.

A los símbolos $\exists$ y $\forall$ se les llama *cuantificador existencial* y *cuantificador universal*, respectivamente.

Podemos hacernos la pregunta siguiente: ¿Cuál es la negación de una proposición, como $(\forall x)(p(x))$? Siendo $(\forall x)(p(x))$ equivalente a que el conjunto P definido por $p(x)$ es todo el universal, $P = S$, entonces $\neg(\forall x)(p(x))$ equivaldrá a $P \neq S$, es decir, a que existen elementos del referencial que *no*

[1] Diremos que A es un subconjunto propio de B (notado $A \subset B$) *si* $A \subseteq B \wedge A \neq B$.

cumplen la condición $p(x)$, o sea que existen elementos de S que cumplen la negación de $p(x)$. Resumiendo:

$$\neg((\forall x)(p(x)) \text{ equivale a } (\exists x)(\neg p(x)).$$

Análogamente, siendo $(\exists x)(p(x))$ equivalente a $P \neq \emptyset$, es entonces claro que $\neg((\exists x)(p(x))$ equivaldrá a $P = \emptyset$, *es decir, ningún elemento del referencial cumple* $p(x)$, o lo que es lo mismo, todo elemento del referencial cumple $\neg p(x)$; en consecuencia,

$$\neg((\exists x)(p(x))) \qquad \text{equivale a} \qquad ((\forall x)(\neg p(x))).$$

Ejercicios

1. Tomando como refencial al conjunto de los números reales, halle los conjuntos que definen las condiciones siguientes:

   (a) $(x^2 - 8x + 15)(x + 1) = 0$.

   (b) b) $x^2 - 8x + 15 \geq 0$.

   (c) c) $x^2 < 2$.

2. Resuelva el ejercicio 1. tomando como referencial al conjunto de los enteros $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

3. Resuelva el ejercicio 1. considerando como referencial al conjunto $\{6, 7, 8, 9, \ldots\}$ de todos los números naturales mayores o iguales que 6.

   En cada uno de los tres ejercicios anteriores, anteponga a cada condición o a su negación, un cuantificador adecuado para que se obtenga una proposición verdadera; dé las razones de sus respuestas.

4. Escriba la negación de cada una de las proposiciones siguientes

   (a) Todos los hombres son mortales.

   (b) $(\forall x)(x + 0 = x)$.

   (c) $(\exists x)(\forall y)(x + y > 0)$.

5. Tomando como referencial al conjunto de los números reales, halle una condición $p(x,y)$ en dos variables, tal que:

   (a) $(\exists x)(\forall y)(p(x,y))$ es falsa y

   (b) $(\forall y)(\exists x)(p(x,y))$ sea verdadera.

6. Usando sus conocimientos y su intuición,

   a) Halle todos los subconjuntos del conjunto $\{1, 2, 3\}$

   b) Halle todos los subconjuntos del conjunto $\{1, 2\}$

   c) Halle todos los subconjuntos del conjunto $\{1\}$

   d) Halle todos los subconjuntos del conjunto $\emptyset$.

   e) ¿Podría usted adivinar una relación entre el número de elementos de un conjunto finito y el número de sus subconjuntos?

   *f) ¿Podría usted demostrar por inducción (sobre el número de elementos del conjunto en cuestión) la relación que ha adivinado en el numeral e)?

7. Escriba la negación de cada una de las expresiones siguientes:

   (a) $(\forall x)(p(x) \to q(x))$.

   (b) $(\forall x)(p(x)) \to (\forall x)(q(x))$.

   (c) $(\forall x)(p(x) \to (q(x) \vee r(x)))$.

   (d) $(\exists x)(\forall z)(p(x,z) \wedge q(z))$.

8. Sea S un referencial para una condición $p(x)$. Sea $A \subseteq S$. Definimos $(\forall x \in A)(p(x))$ como $(\forall x)(x \in A \to p(x))$. Análogamente, definimos $(\exists x \in A)(p(x))$ como $(\exists x)(x \in A \wedge p(x))$.
   Demuestre que $\neg[(\forall x \in A)(p(x))] \leftrightarrow (\exists x \in A)(\neg p(x))$ y que $\neg((\exists x \in A)(p(x))) \leftrightarrow (\forall x \in A)(\neg p(x))$.

9. ¿Qué sentido tienen para usted expresiones como

$$(\forall x)(2+3=5), \qquad (\exists x)(2 \cdot 4 = 8)?$$

   ¿Son éstas proposiciones ? ¿Se podría suprimir el cuantificador?

10. De justificaciones a las equivalencias siguientes:

    (a) $(\forall x)(p \wedge q(x)) \leftrightarrow (p \wedge (\forall x)q(x))$.

    (b) $(\forall x)(p \vee q(x)) \leftrightarrow p \vee (\forall x)q(x))$.

    (c) $(\exists x)(p \wedge q(x)) \leftrightarrow p \wedge (\exists x)q(x))$.

    (d) $(\exists x)(p \vee q(x)) \leftrightarrow (p \vee (\exists x)q(x))$.

    Nota: p es una proposición en la cual no aparece x.

11. Escriba en español correcto la negación de las frases siguientes:

    (a) Si las Matemáticas son fáciles, aprobaré el curso.

    (b) Existe un número natural m tal que cualquiera sea el natural n, $m \leq n$.

    (c) Si el costo de vida continúa subiendo, algunos tendremos que dejar la "costumbre burguesa" de comer tres veces al día o trabajar por un cambio de estructuras sociales.

    (d) Todos tenemos problemas y algunos nos dejamos vencer por ellos.

    (e) Todos los gatos son pardos o algunos estamos miopes.

12. Diga dando las razones de sus respuestas, cuáles de las afirmaciones siguientes son verdaderas y cuáles no:

    (a) $\{1,1,2\} \subseteq \{1,2\}$.

    (b) $\{1,2,2\} = \{2,1\}$.

    (c) $a \in \{\{a\}\}$.

    (d) $\emptyset \in \{\emptyset\}$.

    (e) $A \subseteq \emptyset \to A = \emptyset$.

    (f) $\{a\} \in \{\{a\}\}$.

1.3 OPERACIONES ENTRE CONJUNTOS

Queremos en esta sección estudiar algunas de las formas de construir nuevos conjuntos a partir de otros dados; para saber si realmente los conjuntos son diferentes de los dados, debemos responder antes con certeza la pregunta ¿Cuándo dos conjuntos son iguales? nuestra intuición nos dice inmediatamente: "Dos conjuntos son iguales cuando poseen precisamente los mismos elementos", criterio que adoptamos para trabajar de ahora en adelante. Usando el simbolismo introducido, sería:

$$A = B \quad \text{si y sólo si} \quad (\forall x)(x \in A \leftrightarrow x \in B) \tag{1.1}$$

Así, por ejemplo, $\{1, 2\} = \{2, 1\}$, no importando el orden de los elementos.

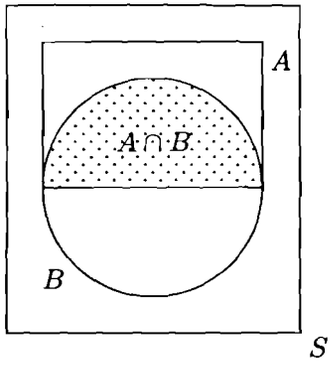
Si en el listado de los estudiantes de un curso se anotase por error dos veces el nombre de uno de los alumnos, con ello no se modificaría el conjunto de estudiantes del curso; en consecuencia $\{1, 2, 3\} = \{1, 2, 1, 3\}$, ya que todo elemento del primer conjunto está en el segundo y recíprocamente, todo elemento del segundo está en el primero, es decir

$$A = B \quad \text{si y sólo si} \quad A \subseteq B \ \wedge \ B \subseteq A \tag{1.2}$$

Si A, B son conjuntos, definimos su *intersección* (notada $A \cap B$) como el conjunto constituido por todos aquellos elementos que pertenecen simultáneamente a A y a B, es decir,

$$A \cap B = \{x \mid x \in A \ \wedge \ x \in B\}$$

Por ejemplo, $\{1, 2, 3, 4, 5, 8\} \cap \{5, 3, 8, 0, 7\} = \{5, 3, 8\}$. Es costumbre visualizar los conjuntos representándolos como regiones planas; a tales gráficas se les llama *diagramas de Venn*. Por ejemplo en el diagrama de Venn adjunto, $A \cap B$ es la parte punteada.



Si A es el conjunto de los enteros pares y B es el de los enteros múltiplos de 3, puede deducirse fácilmente que $A \cap B$ es el conjunto de los enteros múltiplos de 6. Si sucede que $A \cap B = \emptyset$, los conjuntos no poseen elementos comunes y se dice que son *disyuntos*. Las igualdades $A \cap B = B \cap A$, $A \cap \emptyset = \emptyset$, $(A \cap B) \cap C = A \cap (B \cap C)$, $A \cap A = A$, se deducen inmediatamente de las propiedades correspondientes del conectivo "$\wedge$" y de las definiciones; por ejemplo, mostremos que: $(A \cap B) \cap C = A \cap (B \cap C)$

$$\begin{aligned}
x \in (A \cap B) \cap C &\leftrightarrow x \in (A \cap B) \wedge x \in C && \text{[Def. de "}\cap\text{"]} \\
&\leftrightarrow (x \in A \ \wedge \ x \in B) \ \wedge \ x \in C && \text{[Def. de "}\cap\text{"]} \\
&\leftrightarrow x \in A \ \wedge \ (x \in B \ \wedge \ x \in C) && \text{[asociativ. de "}\wedge\text{"]} \\
&\leftrightarrow x \in A \ \wedge \ x \in B \cap C && \text{[Def. de "}\cap\text{"]} \\
&\leftrightarrow x \in A \cap (B \cap C) && \text{[Def. de "}\cap\text{"]}
\end{aligned}$$

Es decir $(\forall x)[x \in (A \cap B) \cap C \leftrightarrow x \in A \cap (B \cap C)]$ lo cual según (1) prueba que $(A \cap B) \cap C = A \cap (B \cap C)$. Mostremos que $A \cap \emptyset = \emptyset$: cualquiera sea x,

$$\begin{aligned}
x \in A \cap \emptyset &\leftrightarrow x \in A \ \wedge \ x \in \emptyset && \text{[Def. de "}\cap\text{"]} \\
&\leftrightarrow x \in \emptyset && \text{[Debido a que siendo } x \in \emptyset \text{ falsa,} \\
& && p \wedge (x \in \emptyset) \text{ es falsa sin importar} \\
& && \text{que } p \text{ sea verdadera o falsa].}
\end{aligned}$$

Nuevamente por (1) se deduce que $A \cap \emptyset = \emptyset$.

Utilizando el conectivo "$\vee$" definiremos la operación entre conjuntos llamada *unión*: si A, B son conjunto cualesquiera la unión de A y B notada $A \cup B$ es el conjunto constituido por todos aquellos elementos que o bien pertenecen solamente a A, o bien pertenecen solamente a B, o pertenecen a A y a B simultáneamente, es decir recordando la tabla de verdad para definir el conectivo "$\vee$",

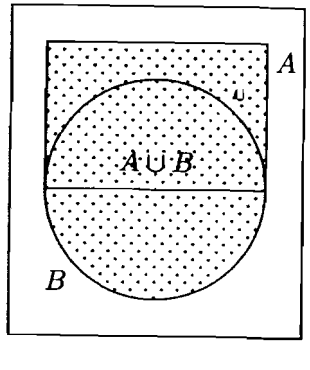
$$A \cup B = \{x \mid x \in A \ \vee \ x \in B\}.$$

Si $A = \{1, 2, 3, 4, 5\}$ y $B = \{4, 5, 0, 6, 7, 8, 9\}$

$$A \cup B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Por ejemplo en el siguiente diagrama, la parte punteada corresponde a la

unión de los conjuntos.



Es sencillo demostrar que $A \cup B = B \cup A, (A \cup B) \cup C = A \cup (B \cup C)$, $A \cup \emptyset = A$ y que $A \cup A = A$. Por ejemplo si usamos la tautología $p \vee p \leftrightarrow p$, se tiene que cualquiera sea x, $x \in A \vee x \in A \leftrightarrow x \in A$, lo cual según la definición de "$\cup$" significa $x \in A \cup A \leftrightarrow x \in A$, cualquiera sea x, es decir $A \cup A = A$. Utilizando tautologías que ligan "$\wedge$"con "$\vee$" puede demostrarse que :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

(distributividad de cada una con respecto a la otra).

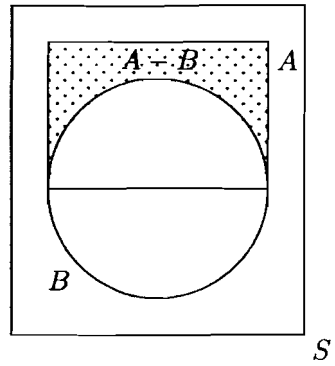
Otra operación de utilidad entre conjuntos es la llamada *diferencia*: Si A, B son conjuntos, por $A - B$ (léase A menos B) designamos al conjunto constituido por los elementos de A que no están en B.

$$A - B = \{x \mid x \in A \wedge x \notin B\} = \{x \in A \mid x \notin B\}.$$

Por ejemplo,

$$\{2,3,7,5,4\} - \{0,5,1,3,8\} = \{2,7,4\} \text{ y}$$
$$\{0,5,1,3,8\} - \{2,3,7,5,4\} = \{0,1,8\}.$$

En el diagrama, $A - B$ es la parte punteada.

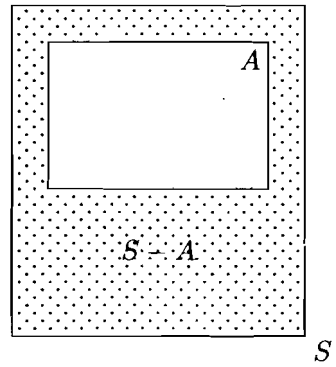


Es fácil demostrar que $A - \emptyset = A$, $A - A = \emptyset$, $A \cap (B - A) = \emptyset$ y $A \cup B = A \cup (B - A)$. Por ejemplo para cualquier x,

$$x \in A - A \leftrightarrow x \in A \wedge x \notin A \qquad \text{[Def. de diferencia]}$$
$$\leftrightarrow x \in A \wedge \neg(x \in A) \qquad \text{la cual es siempre falsa}$$

puesto que tiene la forma de la contradicción $p \wedge (\neg p)$, es decir, no existe un elemento x que pertenezca a $A - A$ o sea que $A - A = \emptyset$ ya que $x \in A \wedge \neg(x \in A)) \leftrightarrow x \in \emptyset$.

Si tomamos un conjunto referencial S (sólo trabajaremos con subconjuntos de S), al conjunto $S - A$ se le acostumbra llamar el *complemento* de A con respecto a S y se nota $C_S A$ o simplemente CA si no hay lugar a confusión.



Es sencillo demostrar que:

$$C(A \cup B) = (CA) \cap (CB) \qquad \text{y que}$$
$$C(A \cap B) = (CA) \cup (CB),$$

igualdades llamadas *leyes de De Morgan*; mostremos la primera y dejemos al lector como ejercicio la segunda:

$$
\begin{aligned}
& x \in C_S(A \cup B) \\
& \leftrightarrow x \in S \ \wedge \ x \notin A \cup B && \text{[Def. de diferencia]} \\
& \leftrightarrow x \in S \ \wedge \ \neg(x \in A \cup B) && \text{[Def. de } \notin\text{]} \\
& \leftrightarrow x \in S \ \wedge \ \neg(x \in A \vee \ x \in B) && \text{[Def. de reunión]} \\
& \leftrightarrow x \in S \ \wedge \ (\neg(x \in A) \wedge \ \neg(x \in B)) && \text{[Tautol. 18, sección 1]} \\
& \leftrightarrow (x \in S \ \wedge \ x \in S) \wedge \ (x \notin A \wedge \ x \notin B) && \text{[Tautol. 1 de la sección 1]} \\
& \leftrightarrow (x \in S \ \wedge \ x \notin A) \wedge \ (x \in S \wedge \ x \notin B) && \text{[Conmutat. y Asociat. de "}\wedge\text{"]} \\
& \leftrightarrow x \in C_S A \ \wedge \ x \in C_S B && \text{[Def. de complemento]} \\
& \leftrightarrow x \in (C_S A) \ \cap \ (C_S B) && \text{[Def. de intersección],}
\end{aligned}
$$

quedando demostrado.

Hemos definido lo que significa "ser un subconjunto de"; tomemos un conjunto S y pensemos en los subconjuntos de S; nuestra intuición nos dice que podemos formar un nuevo conjunto con todos los subconjuntos de S como elementos; por ejemplo si $S = \{a,\ b,\ c\}$, dicho nuevo conjunto, notado $\mathcal{P}(S)$, será

$$\mathcal{P}(S) = \{\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{a,b\},\ \{a,c\},\ \{b,c\},\ S\}.$$

En general, si S es cualquier conjunto, la colección de todos sus subconjuntos o partes, notada $\mathcal{P}(S)$ (léase "partes de S") es $\mathcal{P}(S) = \{A | A \subseteq S\}$.

Como $\emptyset$ es subconjunto de todo conjunto, siempre $\emptyset \in \mathcal{P}(S)$ y como todo conjunto es subconjunto de sí mismo, $S \in \mathcal{P}(S)$. Así $\mathcal{P}(\{a\}) = \{\emptyset,\ \{a\}\}$ y $\mathcal{P}(\emptyset) = \{\emptyset\}$.

Nótese que $\{\emptyset\} \neq \{\ \} = \emptyset$ ya que $\{\emptyset\}$ posee un elemento y en consecuencia no es vacío.

El lector, como ejercicio, puede formar $\mathcal{P}(S)$ para cuando S posee dos, cuatro y cinco elementos; juntando sus resultados con los ejemplos que hemos dado (casos en los cuales S posee cero, uno y tres elementos), puede intuir que "si un conjunto *posee n elementos*, entonces tiene 2^n subconjuntos". Esta propiedad puede probarse usando inducción matemática [1]. Ya se comprobó que es cierta si el conjunto posee 0, 1, 2, 3, 4 y 5 elementos.

[1] Aun cuando posteriormente se estudiará en detalle la inducción matemática, la suponemos conocida por el lector.

Supongamos que se cumple para cuando un conjunto posee n elementos, y demostremos que también vale cuando un conjunto posee $n+1$ elementos:

Sea M un conjunto con $n+1$ elementos; como M no es vacío (¿por qué?) tomemos un elemento b de M y consideremos las dos colecciones siguientes: $\mathfrak{B}$ formada por todos los subconjuntos de M a los cuales pertenece b, y $\mathfrak{A}$ constituida por los subconjuntos de M que no contienen al elemento b, es decir, $\mathfrak{A} = \mathcal{P}(M - \{b\})$; como $M - \{b\}$ posee n elementos, la hipótesis de inducción nos permite afirmar que $\mathfrak{A}$ posee 2^n elementos. Pero para todo conjunto B de $\mathfrak{B}$ existe un único A de $\mathfrak{A}$ tal que $A \cup \{b\} = B$, es decir que $\mathfrak{B}$ se obtiene añadiendo b a cada uno de los conjuntos de $\mathfrak{A}$, y recíprocamente, $\mathfrak{A}$ se obtiene quitando b de cada uno de los conjuntos $\mathfrak{B}$, lo cual significa que $\mathfrak{B}$ posee tantos elementos como $\mathfrak{A}$ (también 2^n). Si además tenemos en cuenta que $\mathfrak{A}$ y $\mathfrak{B}$ son disyuntos y que $\mathcal{P}(M) = \mathfrak{A} \cup \mathfrak{B}$, entonces el número de elementos de $\mathcal{P}(M)$ es igual al número de elementos de $\mathfrak{A}$ sumado con el número de elementos de $\mathfrak{B}$, o sea que es $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$, con lo cual queda demostrado que la propiedad en cuestión también vale para conjuntos con $n+1$ elementos, y por inducción se concluye que vale para todo número natural.

Queremos ahora destacar las íntimas relaciones existentes entre las operaciones con conjuntos definidos por comprensión y los conectivos, para usarlas luego en la justificación de las propiedades usuales de los cuantificadores.

Sean S un referencial, $p(x)$ y $q(x)$ condiciones aplicables a los elementos de S y sean

$$P = \{x \in S \mid p(x)\} \qquad \text{y} \qquad Q = \{x \in S \mid q(x)\}.$$

Dado cualquier elemento de S, siempre podremos decidir si cumple o no con las condiciones anteriores, siendo entonces evidente que

$$\{x \in S \mid \neg p(x)\} = S - P = C_S P.$$

O sea que los elementos que no satisfacen $p(x)$, verifican su negación.

De la simple definición, $P \cap Q$ estará constituido por los elementos de S que están simultáneamente en P y Q, es decir que satisfacen simultáneamente las condiciones $p(x)$ y $q(x)$ que determinan los conjuntos , o sea que

$$\{x \in S \mid p(x)\} \ \cap \ \{x \in S \mid q(x)\} \ = \ \{x \in S \mid p(x) \ \wedge \ q(x)\}.$$

Análogamente,

$$\{x \in S \mid p(x)\} \ \cup \ \{x \in S \mid q(x)\} \ = \ \{x \in S \mid p(x) \ \vee \ q(x)\}.$$

¿Cuál es $\{x \mid p(x) \to q(x)\}$?

Si observamos la tabla de verdad de la implicación, nos damos cuenta que $p(x) \to q(x)$ es verdadera cuando $p(x)$ y $q(x)$ son verdaderas, o cuando $p(x)$ es falsa y $q(x)$ es verdadera o cuando $p(x)$ es falsa y $q(x)$ también lo es; en otras palabras, $p(x) \to q(x)$ es verdadera cuando x está en $P \cap Q$, o cuando x está en $CP \cap Q$ o cuando x está en $CP \cap CQ$. Esto significa que

$$\begin{aligned}\{x \mid p(x) \to q(x)\} &= (P \cap Q) \cup [(CP \cap Q) \cup (CP \cap CQ)] \\ &= (P \cap Q) \cup [CP \cap (Q \cup CQ)] \\ &= (P \cap Q) \cup [CP \cap S] \\ &= (P \cap Q) \cup CP = (P \cup CP) \cap (Q \cup CP) \\ &= S \cap (Q \cup CP) \\ &= (CP) \cup Q.\end{aligned}$$

A este mismo resultado se habría llegado más rápidamente si hubiésemos observado que la implicación es verdadera cuando el antecedente es falso o cuando el consecuente es verdadero. También si hubiéramos recordado que

$$(p(x) \to q(x)) \leftrightarrow (\neg p(x) \ \vee \ q(x))$$

y a la fórmula de la derecha le hubiésemos aplicado los resultados acabados de establecer. Sin embargo creemos que valió la pena hacer la simplificación anterior como ejemplo del uso de las operaciones entre conjuntos.

Ejercicios

1. Pruebe que
   (a) $A \subseteq A \cup B$.
   (b) $A \cap B \subseteq A$.
   (c) Si $A \subseteq B$, entonces $A \cup M \subseteq B \cup M$ para cualquier M.
   (d) d) Si $A \subseteq B$ entonces $A \cap M \subseteq B \cap M$ para cualquier M.
2. Puede suceder que $A \cap B = B$; dé un ejemplo en el cual se cumpla dicha igualdad. ¿Podría idear (demostrándola) una condición necesaria y suficiente para que tal igualdad se cumpla?
3. Se pide lo mismo que en 2. pero con respecto a $A \cup B = A$.

4. Demuestre que si $A \subseteq B$ y $B \subseteq C$ entonces $A \subseteq C$ y que si $M \subseteq N$ entonces $\mathcal{P}(M) \subseteq \mathcal{P}(N)$.
5. Pruebe que
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad \text{y que}$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$
6. Demuestre que $A \cap B = A$ si y solo si $A \subseteq B$ y que $A \cup B = A$ si y solo si $B \subseteq A$.
7. Sea S un conjunto referencial y sean A, B subconjuntos de S. Demuestre que
$$A - B = A \cap (C_S B)$$
Concluya que $(A - B) \subseteq A$.
8. Puede suceder que $A - B = \emptyset$; dé dos ejemplos en los cuales se cumpla dicha igualdad e idee (demostrándola) una condición necesaria y suficiente para que tal igualdad se cumpla.
9. Sean $A_1, A_2, \ldots, A_n$ conjuntos. Pruebe que si $(A_1 \subseteq A_2)$ y $(A_2 \subseteq A_3)$ y $\ldots$ y $(A_{n-1} \subseteq A_n)$ y $A_n \subseteq A_1$, entonces $A_1 = A_2 = \ldots = A_n$.
10. Sean P, Q subconjuntos de un referencial S. Demuestre que
$$P \subseteq Q \qquad \text{si y solo si} \qquad (C_S Q) \subseteq (C_S P).$$
11. Demuestre que $A - (B - C) = (A - B) \cup (A \cap C)$. Según el ejercicio 1, $(A - B) \cup (A \cap C) \supseteq A - B$ y según la parte final del ejercicio 7. $(A - B) \supseteq (A - B) - C$; concluya que $A - (B - C) \supseteq (A - B) - C$ y dé un contraejemplo para mostrar que en general no vale la contenencia en el sentido contrario.
12. Muestre que
$$A \cap (B - C) = (A \cap B) - (A \cap C)$$
$$A \cup (B - C) = (A \cup B) - (C - A)$$
pero que en general la unión no es distributiva respecto de la diferencia.
13. Definimos una nueva operación entre conjuntos llamada la *diferencia simétrica* así:
$$A \triangle B = \{x \mid x \in A \veebar x \in B\}$$

(a) Usando la tautología 15) de la sección 1, pruebe la asociatividad de la diferencia simétrica: $(A \triangle B) \triangle C = A \triangle (B \triangle C)$. Represente estos conjuntos en un diagrama de Venn.

(b) Demuestre que $A \triangle B = (A - B) \cup (B - A)$.

(c) Pruebe que la diferencia simétrica es conmutativa.

(d) Pruebe que $A \triangle B = A \cup B - (A \cap B)$.

(e) Usando diagramas de Venn y luego prescindiendo de ellos, halle $A \triangle \emptyset$, $A \triangle A$ y $A \triangle B$ si $A \subseteq B$.

(f) Sea S un conjunto referencial y consideremos "$\triangle$" actuando solamente entre subconjuntos de S; demuestre que se cumplen las propiedades siguientes :

$$(\exists M \in \mathcal{P}(S))(\forall A \in \mathcal{P}(S))(A \triangle M = A)$$
$$(\forall A \in \mathcal{P}(S))(\exists B \in \mathcal{P}(S))(A \triangle B = \emptyset)$$

Concluya que $\mathcal{P}(S)$ con "$\triangle$" como operación cumple con las condiciones llamadas de "grupo conmutativo"[1].

(g) Pruebe que la intersección es distributiva con respecto a la diferencia simétrica.

14. ¿Cumple $\mathcal{P}(S)$ con la unión como operación, con las condiciones de grupo conmutativo? ¿Las cumple $\mathcal{P}(S)$ con la intersección como operación?
Dé las razones de sus respuestas.

15. Pruebe que $(P \cap Q) \cup (CP \cap CQ) = (CP \cup Q) \cap (P \cup CQ)$.

16. Usando las mismas notaciones de la sección anterior halle

$$\{x \in S | p(x) \leftrightarrow q(x)\}.$$

17. Sean, A y B conjuntos cualesquiera; pruebe que A y $B - A$ son disyuntos y que $A \cup B = A \cup (B - A)$.

[1]Si el lector no sabe lo que es un grupo conmutativo, puede enterarse consultando un libro de álgebra abstracta o moderna.

1.4 CONECTIVOS Y CUANTIFICADORES

En esta sección queremos poner de presente las relaciones existentes entre los conectivos y los cuantificadores, es decir, las reglas que rigen el comportamiento de los cuantificadores con respecto a los conectivos. Ya conocemos las de la negación :

C1 : $\neg(\forall x p(x)) \leftrightarrow \exists x(\neg p(x))$.

C2: $\neg(\exists x p(x)) \leftrightarrow \forall x(\neg p(x))$.

Veamos las demás; en cuanto a la conjunción, tenemos;

C3 : $\forall x(p(x) \wedge q(x)) \leftrightarrow (\forall x p(x) \wedge \forall x q(x))$.

o sea que "$\forall$" distribuye con respecto a "$\wedge$". El comportamiento de "$\exists$" no es tan bueno:

C4 : $\exists x(p(x) \wedge q(x)) \rightarrow (\exists x p(x) \wedge \exists x q(x))$.

pero la *implicación recíproca no es válida.*

Con la disyunción sucede lo contrario, ya que "$\exists$" distribuye con respecto a ella pero no así "$\forall$":

C5 : $\exists x(p(x) \vee q(x)) \leftrightarrow ((\exists x p(x) \vee (\exists x q(x)))$.

C6 : $(\forall x p(x) \vee \forall x q(x)) \rightarrow \forall x(p(x) \vee q(x))$.

mas *no vale la implicación recíproca.*

Para la implicación solo se tienen implicaciones:

C7 : $\forall x(p(x) \rightarrow q(x)) \rightarrow (\forall x p(x) \rightarrow \forall x q(x))$.

C8 : $(\exists x p(x) \rightarrow \exists x q(x)) \rightarrow \exists x(p(x) \rightarrow q(x))$.

pero *no valen las implicaciones recíprocas.*

Para la equivalencia es fácil deducir de C7 y C8 otras dos propiedades similares:

C9 : $\forall x(p(x) \leftrightarrow q(x)) \rightarrow (\forall x p(x) \leftrightarrow \forall x q(x))$.

C10 : $(\exists x p(x) \leftrightarrow \exists x q(x)) \rightarrow \exists x(p(x) \leftrightarrow q(x))$.

y *tampoco valen las implicaciones recíprocas.*

A continuación justificaremos algunas de las relaciones anteriores y dejaremos como trabajo para el lector el hacerlo para las restantes.

Recordemos que dado un referencial S cualquiera y condiciones $p(x)$, $q(x)$ adecuadas (relativas a los elementos de S), hemos definido $\exists x p(x)$ como $\{x \in S \mid p(x)\} \neq \emptyset$ y $\forall x p(x)$ como $\{x \in S \mid p(x)\} = S$. Las "demostraciones" de C3 a C10 pueden hacerse utilizando estas definiciones junto con las relaciones ya vistas entre conectivos y operaciones sobre conjuntos.

Por ejemplo, justifiquemos C3:
Supongamos que $\forall x(p(x) \wedge q(x))$ es cierta; esto equivale a
$\{x \in S \mid p(x) \wedge q(x)\} = S$; pero

$$\{x \in S \mid p(x) \wedge q(x)\} = \{x \in S \mid p(x)\} \cap \{x \in S \mid q(x)\}$$

y esta intersección es todo el referencial S si y sólo si cada conjunto intersecante es el referencial:

$$P = \{x \in S \mid p(x)\} = S \qquad \text{y} \qquad Q = \{x \in S \mid q(x)\} = S$$

o sea que $\forall x p(x) \wedge \forall x q(x)$ es cierta. Como todas las afirmaciones hechas son equivalentes, se obtiene el resultado deseado.

Procedamos a establecer C4: Supongamos que $\exists x(p(x) \wedge q(x))$; esto significa que

$$\{x \in S \mid p(x) \wedge q(x)\} \neq \emptyset$$

lo cual equivale a $P \cap Q \neq \emptyset$; de aquí se sigue que $P \neq \emptyset$ y $Q \neq \emptyset$ (pues si al menos uno fuese vacío, su intersección también lo sería), o sea que

$$\exists x p(x) \wedge \exists x q(x)$$

Para refutar la implicación recíproca, basta hallar un conjunto referencial S adecuado y condiciones específicas $p(x)$ y $q(x)$ para las cuales *no se pueda tener* $(\exists x p(x) \wedge \exists x q(x)) \rightarrow \exists x(p(x) \wedge q(x))$. Es suficiente hallar un contraejemplo, ya que se sobrentiende que C1 a C10 valen para todos los referenciales y para todas las condiciones $p(x)$, $q(x)$.

Tomemos como referencial al conjunto $\mathbb{Z}$ de los enteros y como condiciones $p(x)$: x es par y $q(x)$: x es impar. En esta forma la proposición $\exists x p(x) \wedge \exists x q(x)$ es cierta ya que existen enteros pares y enteros impares; sin embargo $\exists x(p(x) \wedge q(x))$ es falsa ya que está afirmando la existencia de un entero que es par e impar simultáneamente.

Establezcamos C5 utilizando C1 y C3: Como C3 vale para condiciones cualesquiera, también deberá tenerse para $\neg p(x)$ y $\neg q(x)$, es decir,

$$\forall x((\neg p(x)) \wedge (\neg q(x))) \leftrightarrow (\forall x(\neg p(x)) \wedge \forall x(\neg q(x)))$$

Pero si estas dos proposiciones son equivalentes, también lo son sus negaciones

$$\neg[\forall x((\neg p(x)) \wedge (\neg q(x)))] \leftrightarrow \neg[\forall x(\neg p(x)) \wedge \forall x(\neg q(x))]$$

Aplicando C1 y las tautologías 13 y 5 de la sección 1, se obtiene el resultado:

$$[\exists x \neg((\neg p(x)) \wedge (\neg q(x)))] \leftrightarrow [\neg \forall x(\neg p(x)) \vee \neg \forall x(\neg q(x))]$$
$$\exists x(\neg\neg p(x)) \vee \neg\neg q(x)) \leftrightarrow [\exists x(\neg\neg p(x)) \vee \exists x(\neg\neg q(x))]$$

o sea $$\exists x[p(x) \vee q(x)] \leftrightarrow [\exists x p(x) \vee \exists x q(x)]$$

Probemos a continuación C7: $\forall x(p(x) \rightarrow q(x)) \rightarrow (\forall x p(x) \rightarrow \forall x q(x))$.

Supongamos S, $p(x)$, y $q(x)$ bajo las mismas hipótesis anteriores. Según la tautología 10 de la §1, la fórmula C7 es equivalente a

$$[(\forall x(p(x) \rightarrow q(x))) \wedge (\forall x p(x))] \rightarrow [\forall x q(x)]$$

así que podemos probarla en lugar de la original, para lo cual, según la tabla de verdad de la implicación, es suficiente demostrar que si el antecedente es verdadero, también lo es el consecuente. Supongamos que en efecto $(\forall x(p(x) \rightarrow q(x))) \wedge (\forall x p(x))$ es verdadero; según la definición de "$\wedge$", las dos serán proposiciones verdaderas y de acuerdo con la definición del cuantificador universal, sus respectivos conjuntos solución serán todo el universal, es decir

$$\{x \in S \mid p(x) \rightarrow q(x)\} = S \quad \text{y} \quad P = \{x \in S \mid p(x)\} = S.$$

Según la tautología 14 de la sección 1, el primer conjunto será

$$\begin{aligned} S &= \{x \in S \mid (\neg p(x)) \vee q(x)\} \\ &= \{x \in S \mid \neg p(x)\} \cup \{x \in S | q(x)\} \\ &= (S - P) \cup Q. \end{aligned}$$

Pero $P = S$, de donde $S - P = \emptyset$, luego

$$S = \emptyset \cup Q = Q$$

o sea que $(\forall x q(x))$ es verdadera, quedando probado lo propuesto.

Ejercicios

1. Establezca las propiedades C6, C8, C9 y C10 anteriores, ya sea utilizando conjuntos o usando resultados ya obtenidos.

2. Pruebe o refute la afirmación

$$\forall x \neg p(x) \rightarrow \neg \forall x p(x)$$

¿Es verdadera o falsa la implicación recíproca?

3. Dé contraejemplos adecuados para mostrar que no valen las implicaciones recíprocas de C6, C7 y C8.

4. Pruebe o refute: $\forall x p(x) \rightarrow \exists x p(x)$.

5. Dé una justificación a la implicación

$$(\exists x)(\forall y)(p(x,y)) \rightarrow (\forall y)(\exists x)(p(x,y)).$$

6. Dé dos contraejemplos para mostrar que en general no se cumple la implicación recíproca de 5.

1.5 COLECCIONES DE CONJUNTOS

Hemos definido la intersección, la unión, la diferencia y la diferencia simétrica de *dos* conjuntos, usando algunos de los conectivos proposicionales. Queremos extender la intersección y la unión a colecciones de conjuntos, destacando el papel que en tales operaciones juegan los cuantificadores.

Si A_1, A_2, A_3 son conjuntos, $(A_1 \cap A_2) \cap A_3 = A_1 \cap (A_2 \cap A_3)$, de modo que se puede definir $A_1 \cap A_2 \cap A_3$ como cualquiera de los miembros de la anterior igualdad. Análogamente, si A_1, A_2, A_3, A_4 son conjuntos, podemos definir $A_1 \cap A_2 \cap A_3 \cap A_4$ como $((A_1 \cap A_2) \cap A_3) \cap A_4)$, o como $A_1 \cap (A_2 \cap (A_3 \cap A_4))$, o como $(A_1 \cap A_3) \cap (A_2 \cap A_4)$, por ejemplo, ya que por las propiedades asociativa y conmutativa de la intersección (o de "$\wedge$", si se prefiere) se puede demostrar que todos estos conjuntos son iguales. Generalizando: si se tiene una colección $\mathfrak{C}$ de conjuntos, la intersección de los conjuntos de $\mathfrak{C}$ estará formada por aquellos elementos que pertenecen a *todos* los conjuntos de $\mathfrak{C}$, sin importar el orden en el cual se dispongan los conjuntos de $\mathfrak{C}$; dicha interseción se acostumbra notar $\bigcap_{A \in \mathfrak{C}} A$ ó $\bigcap \mathfrak{C}$. Resumiendo:

$$\bigcap_{A \in \mathfrak{C}} A = \{x \mid (\forall A \in \mathfrak{C})(x \in A)\}$$

Por ejemplo, si para cada natural $n \geq 2$ se define $A_n = (-\frac{1}{n}, 3 + \frac{1}{n})$ y $\mathfrak{C}$ es la colección de todos estos conjuntos, entonces

$$\bigcap_{A_n \in \mathfrak{C}} A_n = \bigcap_{n=2}^{\infty} A_n = [0,3],$$

como puede observarlo el lector dando valores a n y representando los A_n sobre una recta.

De manera semejante al caso de la intersección, si A_1, A_2, A_3, A_4 son conjuntos cualesquiera, $A_1 \cup A_2 \cup A_3 \cup A_4$, puede definirse como $A_1 \cup (A_2 \cup (A_3 \cup A_4))$, o como $(A_1 \cup A_2) \cup (A_3 \cup A_4)$, o como $(A_4 \cup A_2) \cup (A_3 \cup A_1)$, etc.; lo esencial está en que $A_1 \cup A_2 \cup A_3 \cup A_4$ está formado por todos aquellos elementos que pertenecen al menos a uno de los conjuntos dados; si $\mathfrak{C}$ es una colección cualquiera de conjuntos, la unión de $\mathfrak{C}$, es decir la unión de todos los conjuntos de $\mathfrak{C}$, notada $\bigcup \mathfrak{C}$ ó $\bigcup_{A \in \mathfrak{C}} A$, está constituida por todos aquellos elementos que pertenecen al menos a uno de los conjuntos de $\mathfrak{C}$; dicho de otra manera,

$$\bigcup \mathfrak{C} = \bigcup_{A \in \mathfrak{C}} A = \{x \mid (\exists A \in \mathfrak{C})(x \in A)\}$$

Por ejemplo, si para cada natural $n \geq 2$, se define $A_n = [\frac{1}{n}, 1 - \frac{1}{n}]$ y $\mathfrak{C}$ es la colección de estos conjuntos ($\mathfrak{C} = \{A_n | n \geq 2\}$), entonces

$$\bigcup \mathfrak{C} = \bigcup_{A_n \in \mathfrak{C}} A_n = \bigcup_{n=2}^{\infty} A_n = (0,1)$$

como puede verse representando los A_n sobre una recta.

Demostremos ahora la siguiente propiedad de asociatividad de la intersección: Si $\mathfrak{A}$ y $\mathfrak{B}$ son colecciones de conjuntos y $\mathfrak{C} = \mathfrak{A} \cup \mathfrak{B}$

$$\bigcap_{A \in \mathfrak{C}} A = \left(\bigcap_{A \in \mathfrak{A}} A\right) \cap \left(\bigcap_{A \in \mathfrak{B}} A\right)$$

En efecto:

$x \in \bigcap_{A \in \mathfrak{C}} A \leftrightarrow (\forall A \in \mathfrak{C})(x \in A)$ [Def. de interseción.]

$\leftrightarrow (\forall A)(A \in \mathfrak{C} \rightarrow x \in A)$ [Def. del cuant. localizado]

$\leftrightarrow (\forall A)((A \in \mathfrak{A} \cup \mathfrak{B}) \rightarrow x \in A)$ [Def. de $\mathfrak{C}$]

$\leftrightarrow (\forall A)((A \in \mathfrak{A} \vee A \in \mathfrak{B}) \rightarrow x \in A)$ [Def. de "$\cup$"]

$\leftrightarrow (\forall A)(\neg(A \in \mathfrak{A} \vee A \in \mathfrak{B}) \vee x \in A)$ [tautología 14 de la sec. 1]

$\leftrightarrow (\forall A)((A \notin \mathfrak{A} \wedge A \notin \mathfrak{B}) \vee x \in A)$ [tautología 17 de la sec. 1]

$\leftrightarrow (\forall A)((A \notin \mathfrak{A} \vee x \in A) \wedge (A \notin \mathfrak{B} \vee x \in A))$ [distributividad]

$\leftrightarrow (\forall A)((A \in \mathfrak{A} \rightarrow x \in A) \wedge (A \in \mathfrak{B} \rightarrow x \in A))$ [tautología 14]

$\leftrightarrow (\forall A)((A \in \mathfrak{A} \rightarrow x \in A) \wedge (\forall A)(A \in \mathfrak{B} \rightarrow x \in A))$ [ejer. 13, sec. 3]

$\leftrightarrow x \in \bigcap_{A \in \mathfrak{A}} A \wedge x \in \bigcap_{A \in \mathfrak{B}} A$ [Def. de inters. de colecciones]

$\leftrightarrow x \in \left(\left(\bigcap_{A \in \mathfrak{A}} A\right) \cap \left(\bigcap_{A \in \mathfrak{B}} A\right)\right)$ [Def. de "$\cap$"]

Con lo cual queda demostrada la igualdad.

Si $\mathfrak{C}$ es una colección cualquiera de conjuntos y M es cualquier otro

conjunto, se tiene que

$$M \cap \left(\bigcup_{A \in \mathfrak{C}} A\right) = \bigcup_{A \in \mathfrak{C}} (M \cap A) \quad \text{y}$$

$$M \cup \left(\bigcap_{A \in \mathfrak{C}} A\right) = \bigcap_{A \in \mathfrak{C}} (M \cup A).$$

La primera es la distributividad de la intersección con respecto a la unión y la segunda la de la unión con respecto a la intersección de una colección de conjuntos. Dejamos sus demostraciones al lector (ver ejercicio 6 de esta sección) .

Para colecciones de conjuntos, las leyes de De Morgan vienen a ser

$$C_S\left(\bigcup_{A \in \mathfrak{C}} A\right) = \bigcap_{A \in \mathfrak{C}} (C_S A)$$

$$C_S\left(\bigcap_{A \in \mathfrak{C}} A\right) = \bigcup_{A \in \mathfrak{C}} (C_S A)$$

o de manera más general, si M es un conjunto cualquiera y $\mathfrak{C}$ es una colección de conjuntos (no necesariamente de subconjuntos de M), entonces

$$M - \left(\bigcup_{A \in \mathfrak{C}} A\right) = \bigcap_{A \in \mathfrak{C}} (M - A)$$

$$M - \left(\bigcap_{A \in \mathfrak{C}} A\right) = \bigcup_{A \in \mathfrak{C}} (M - A)$$

Observación: Si $\mathfrak{C}^*$ es la colección de los complementos de los conjuntos de $\mathfrak{C}$, en vez de $\bigcap \mathfrak{C}^*$ hemos escrito $\bigcap_{A \in \mathfrak{C}} C_S A$, notación muy usada; una notación análoga se ha adoptado en las otra igualdades anteriores y se seguirá empleando sin previo aviso.

Demostremos que

$$M - (\bigcup_{A \in \mathfrak{C}} A) = \bigcap_{A \in \mathfrak{C}} (M - A):$$

cualquiera sea x,

$x \in M - (\bigcup_{A\in\mathfrak{C}} A) \leftrightarrow$

$\leftrightarrow x \in M \ \wedge \ \neg\left(x \in \bigcup_{A\in\mathfrak{C}} A\right)$ [Def. de diferencia]

$\leftrightarrow x \in M \ \wedge \ \neg((\exists A \in \mathfrak{C})(x \in A))$ [Def. de reunión]

$\leftrightarrow x \in M \ \wedge \ (\forall A \in \mathfrak{C})(x \notin A)$ [Ejercicio 9, sección 2]

$\leftrightarrow (\forall A \in \mathfrak{C})(x \in M \ \wedge \ x \notin A))$ [Ejercicio 11 sección 2 ya que A y $\mathfrak{C}$ no figuran en $x \in M$]

$\leftrightarrow (\forall A \in \mathfrak{C})(x \in M - A)$ [Def. de diferencia]

$\leftrightarrow x \in \bigcap_{A\in\mathfrak{C}} (M - A)$ [Observación anterior y definición de intersección].

De manera análoga el lector probará la otra igualdad.

Ejercicios

1. Demuestre que si $A_n = (-\frac{1}{n}, 3 + \frac{1}{n})$, entonces
$$\bigcap_{n=2}^{\infty} A_n = [0.3]$$

2. Pruebe que si $B_n = [\frac{1}{n}, 1 - \frac{1}{n}]$, entonces
$$\bigcup_{n=2}^{\infty} B_n = (0.1)$$

3. Demuestre que si $(\forall A \in \mathfrak{C})(A \subseteq M)$, entonces
$$\left(\bigcup_{A\in\mathfrak{C}} A\right) \subseteq M.$$

4. Demuestre que si A_0 es cualquier conjunto de una colección no vacía $\mathfrak{C}$, entonces $(\bigcap_{A\in\mathfrak{C}} A) \subseteq A_0$. Use este hecho para concluir que si existe A_0 en $\mathfrak{C}$ tal que $A_0 \subseteq M$, entonces $(\bigcap_{A\in\mathfrak{C}} A) \subseteq M$.

5. Si $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ son colecciones de conjuntos tales que $\mathfrak{C} = \mathfrak{A} \cup \mathfrak{B}$, entonces
$$\bigcup_{A\in\mathfrak{C}} A = \left(\bigcup_{A\in\mathfrak{A}} A\right) \cup \left(\bigcup_{A\in\mathfrak{B}} A\right).$$

6. Demuestre las propiedades de distributividad propuestas en la página 33.

7. Pruebe que si $(\forall A \in \mathfrak{C})(M \subseteq A)$, entonces $M \subseteq \bigcap_{A\in\mathfrak{C}} A$.

8. Si $A_n = \{x \in \mathbb{R} \mid x \geq n\}$, halle
$$\bigcap_{n=2}^{\infty} A_n.$$
Dé la razón de su respuesta.

9. Si $\mathfrak{C} = \{A_1, A_2, \ldots, A_n\}$ es una colección finita de conjuntos, definimos a partir de ella la colección $\bar{\mathfrak{C}} = \{B_1, B_2, \ldots, B_n\}$ en la forma siguiente:
$$B_1 = A_1;\ B_2 = A_2 - A_1;\ B_3 = A_3 - (A_2 \cup A_1);$$
$$\ldots B_k = A_k - (A_1 \cup A_2 \cup \ldots \cup A_{k-1}) \ldots$$
$$B_n = A_n - (A_1 \cup A_2 \cup \ldots \cup A_{n-1}).$$
Pruebe que los conjuntos de $\bar{\mathfrak{C}}$ son disyuntos dos a dos y que
$$B_1 \cup B_2 \cup \ldots \cup B_n = A_1 \cup A_2 \cup \ldots \cup A_n.$$

1.6 ALGUNAS PARADOJAS

Hasta este momento hemos dado los primeros pasos en un desarrollo de la Teoría de Conjuntos de una manera intuitiva; podríamos haber continuado dicho desarrollo hasta obtener en una forma bastante aceptable, prácticamente todos los conocimientos sobre los conjuntos que se necesitarían para trabajar en casi cualquier rama de la matemática. Sin embargo, como un reflejo del desarrollo histórico de este campo, nos detendremos un momento a revisar lo hecho, a preguntarnos si nuestras hipótesis y nuestros métodos de trabajo y raciocinio son correctos, o si dan lugar a conclusiones un tanto preocupantes, que por ejemplo invaliden algunos de los resultados obtenidos.

En matemáticas, la principal regla de deducción, la que tal vez más usamos, es la llamada "*Modus Ponens*" la cual aproximadamente dice lo siguiente "De p y $p \rightarrow q$ se sigue q", es decir, si en una teoría se sabe que tanto p como $p \rightarrow q$ son teoremas, entonces también q es un teorema; esta regla parece bastante natural si meditamos sobre la forma como razonamos. y si observamos que cuando p es verdadera, $p \rightarrow q$ es verdadera si y sólo si q es verdadera.

Ya antes habíamos definido una *contradicción* como una proposición compuesta que es siempre falsa, independientemente de la veracidad de las proposiciones componentes; el prototipo de las contradicciones es $p \wedge (\neg p)$. Supongamos que en una teoría se demuestre una cierta proposición p y posteriormente también se logre probar $\neg p$; habremos demostrado entonces $p \wedge (\neg p)$, es decir habremos obtenido en la teoría una contradicción (tal teoría se llamará *contradictoria* o *inconsistente*); si q es cualquier proposición de la teoría, $(p \wedge (\neg p)) \rightarrow q$ es uno de sus teoremas ya que es una tautología (el lector puede hacer la tabla de verdad), y como se tenía $p \wedge (\neg p)$, entonces por modus ponens deducimos q; si en vez de q hubiéramos tomado $\neg q$, el mismo argumento nos habría permitido deducir $\neg q$, o sea que en tal teoría todas las proposiciones y sus negaciones serían teoremas (intuitivamente, todas las proposiciones serían cierta y falsas simultáneamente), invalidando completamente la teoría. Este es el motivo por el cual la aparición de una sola contradicción causa tanta inquietud, zozobra y desesperación, según nuestra credibilidad en la teoría o según la dependencia que de ella haya tenido nuestro trabajo.

Una de las primeras contradicciones (o paradojas) que surgieron en la teoría de los conjuntos fue la *del mayor cardinal*, descubierta por *George Cantor* en 1899 : en la teoría intuitiva se aceptaba la existencia del conjunto S de todos los conjuntos; nos referimos a *todos* los conjuntos, es decir, a S deben pertenecer todas las cosas, entes, etc. que existan o hayan existido jamás; ningún otro conjunto puede tener más elementos que éste, luego su número de elementos o cardinal ($\#(S)$) es el mayor que existe; en particular (1) $\#(S) \geq \#(\mathcal{P}(S))$. Pero Cantor demostró que para cualquier conjunto M, $\#(\mathcal{P}(M)) > \#(M)$ (Nosotros ya lo probamos para M finito, puesto que $\#(\mathcal{P}(M)) = 2^{\#(M)} > \#(M)$) y en consecuencia (2) $\#(\mathcal{P}(S)) > \#(S)$, proposición esta que es exactamente la negación de (1).

Otra paradoja notable fue la hallada por el filósofo y matemático inglés *Bertrand Russell* a comienzos del presente siglo: En teoría intuitiva de conjuntos, como lo hicimos en la sección 2, un conjunto se puede determinar (por comprensión) dando la condición que deben cumplir sus elementos; es decir, dada una condición $p(x)$, siempre existe el conjunto constituido por los elementos que cumplen $p(x)$; era de esperarse que esta forma tan amplia de determinar conjuntos llevase a contradicciones. Russell ideó una muy sencilla: Una condición legítima y simple en teoría de conjuntos es "no ser elementos de sí mismo": $x \notin x$. De acuerdo con la teoría intuitiva de conjuntos deberá existir el conjunto de aquellos conjuntos que cumplan dicha condición; llamémoslo M.

$$M = \{x : x \notin x\}.$$

¿Es M elemento de sí mismo?

Si lo es, debe cumplir la condición que definió a M, es decir $M \notin M$: en consecuencia,

$$M \in M \rightarrow M \notin M.$$

Si no es elemento de sí mismo, está cumpliendo la condición que define a M, así que deberá pertenecer a M; en consecuencia

$$M \notin M \rightarrow M \in M.$$

Por la ley del tercio excluido se deberá tener necesariamente $M \in M$ o bien $M \notin M$; cualquiera sea el caso, combinando la proposición válida mediante modus ponens con la implicación correspondiente, obtenemos una contradicción.

Analizando detenidamente lo expuesto, se pone de manifiesto que las paradojas anteriores surgieron entre otras razones, debido a que se podían considerar conjuntos sumamente grandes, a que se tenía demasiada libertad en la escogencia de las condiciones que determinan conjuntos, a que el concepto de "condición" no era claro ni preciso y a que "no basta con

pronunciar algunas palabras mágicas (como $x \notin x$) para determinar un conjunto". Como lo hicimos notar en la sección 2, necesitamos de un conjunto referencial a cuyos elementos puedan aplicarse esas palabras.

Las dos paradojas anteriores ilustran una de las clases de contradicciones que surgieron en la teoría de conjuntos, por su naturaleza pudiéramos llamarlas paradojas matemáticas, para distinguirlas de las semánticas o linguísticas originadas en la forma como se usa el lenguaje cotidiano. La más vieja tal vez es la atribuida (siglo VI a.c.) al poeta cretense *Epiménides*: "Todos los cretenses son mentirosos" o mejor "Todas las declaraciones que hacen los cretenses son falsas", afirmación contradictoria al ser Epiménides cretense; escribamos el raciocinio en detalle:

(1) Todas las declaraciones que hacen los cretenses son falsas.

(2) La declaración (1) la hizo un cretense.

(3) Por lo tanto, la declaración (1) es falsa.

(4) En consecuencia, no todas las declaraciones que hacen los cretenses son falsas.

La (1) se contradice a sí misma, ya que si aceptamos (1), como (1) implica (4), por modus ponens debemos aceptar (4).

Algo semejante sucede con la afirmación "No hay regla sin excepciones"; como esta afirmación es una regla, ella debe tener excepciones, luego deberán existir reglas sin excepciones.

Similar a la paradoja de Russell es la originada con el concepto de "heterologicidad". Cada adjetivo del idioma español tiene un significado; algunas veces ese significado puede aplicarse al adjetivo mismo, otras no; así, "polisilábica" es una palabra polisilábica, "verde" no es una palabra verde, "española" es una palabra española, etc. Diremos que un adjetivo es heterológico si no es aplicable a sí mismo. Pero "heterológico" es un adjetivo; si es aplicable a sí mismo, " heterológico" es heterológico, y según la definición, no sería aplicable a sí mismo. Si no es aplicable a sí mismo, entonces dicho adjetivo es heterológico, en otras palabras "heterológico" es heterológico así que sería aplicable a sí mismo.

Notemos que estas paradojas tienen un patrón común: en la primera se hace una afirmación aplicable a sí misma; en la segunda se enuncia una regla aplicable a sí misma y en la última se define un adjetivo aplicable a sí mismo. En "todas las declaraciones que hacen los cretenses son falsas", las "declaraciones" se refieren a cosas, a hechos, pero la afirmación en sí es una declaración acerca de declaraciones con respecto a cosas. En "no hay reglas sin excepciones", las "reglas" a que se hace referencia son reglas acerca de cosas mientras que la regla en sí no es una regla acerca de cosas sino una

regla acerca de *reglas* sobre cosas. Los adjetivos se refieren a propiedades de cosas, mientras que "heterológico" es un adjetivo que se refiere a adjetivos.

No se está haciendo una diferencia entre el lenguaje en le cual se hacen declaraciones acerca de cosas o de relaciones entre cosas (llamado *lenguaje objeto*) y el lenguaje en el cual se hacen afirmaciones sobre las declaraciones acerca de cosas (llamado *metalenguaje*).

La expresión "Bogotá posee cinco millones de habitantes", correspondería al lenguaje objeto, mientras que "La proposición 'Bogotá posee cinco millones de habitantes' es verdadera", correspondería al metalenguaje (y todo el párrafo anterior correspondería al metametalenguaje). Bien habríamos podido redactar en inglés todas las reglas sintácticas del español, constituyéndose así el inglés en un metalenguaje del español.

Las paradojas anteriores hacen ver entre otras cosas que (como lo decía A. Tarski en [10]) todo lenguaje que contenga a su metalenguaje y en el cual las leyes lógicas usuales subsistan, tiene que ser inconsistente.

Además nuestro lenguaje es impreciso y ambiguo; es difícil hallar dos personas que usen una palabra con exactamente el mismo significado; inclusive una misma persona, en distintas épocas de su vida da a las palabras matices y sentidos diferentes.

También, al usar el lenguaje cotidiano en nuestro trabajo, al no poder-nos desprender de los significados intuitivos de las palabras usadas, hacemos muchas veces suposiciones tácitas que invalidan nuestros razonamientos, como le sucedió a Euclides en algunas de las demostraciones que aparecen en sus " Elementos".

Los motivos anteriores hacen ver la necesidad de introducir un lenguaje objeto propio para cada teoría, cuyos símbolos estén un poco desligados de los significados usuales, cuyas expresiones sean lo más precisas posibles, libres de ambigüedades, y cuyo manejo se haga de acuerdo a reglas claras de sintaxis. Nuestro lenguaje cotidiano se considera entonces, con ciertas restricciones, como el metalenguaje de la teoría.

Si se desea hacer un desarrollo de una teoría dentro de lo que se llama el *patrón de la axiomática formal*, la creación del lenguaje propuesto es indispensable, es el primer paso. Dicho lenguaje contendrá símbolos para describir los objetos, las operaciones y las relaciones entre ellos; se considerarán como los símbolos primitivos, indefinidos de la teoría, y los que se introduzcan posteriormente deberán definirse mediante los primitivos.

El desarrollo que haremos en este texto introductorio a la teoría de conjuntos no será formal, pero sí formalizable. Daremos una idea de la manera como se construye un lenguaje y como ejemplo elaboraremos el

correspondiente a nuestra teoría; los axiomas y los teoremas principales los enunciaremos en este lenguaje; también daremos en él algunas demostraciones o partes de ellas, haciendo notar la "suficiencia" de tal lenguaje, pero no lo emplearemos para desarrollar formalmente la teoría por varias razones: la lectura se hace un tanto monótona y hasta difícil, sobre todo en un principio, cuando el lector novato no posee un dominio del nuevo idioma; el estudiante tiende a pensar que este lenguaje es un fin, una meta y no un medio, una simple herramienta de trabajo; otras veces se usa como una especie de taquigrafía, se abusa de él y en estas primeras etapas del aprendizaje al carecerse de su dominio, se dicen barbaridades y se cometen errores peores que aquellos que se querían corregir. Emplearemos entonces una mezcla del lenguaje de la teoría de los conjuntos con el español, precisando eso sí al máximo el sentido con el cual se usarán las expresiones, evitando las contradicciones en una forma tal que un "experto" pueda con relativa facilidad formalizar el desarrollo efectuado.

Ejercicios

1. Presente otros dos ejemplos de paradojas linguísticas, explicando los motivos por los cuales ocurren.

2. Pregunte a cinco personas (y pregúntese a sí mismo ¿Qué es una propiedad? ¿Qué es una condición? Compare las respuestas y analice las diferencias encontradas.

3. ¿Podemos aceptar dentro de los conceptos matemáticos el de amistad?

   Con más precisión, ¿las relaciones "ser amigo de", "amar a" pueden considerarse como relaciones en el sentido matemático?

   ¿Puede usted determinar por extensión los "conjuntos"

   $\{x \mid x$ es hoy amigo del actual presidente de Ecuador$\}$,

   $\{x \mid x$ es revolucionario$\}$,

   $\{x \mid x$ ama el trabajo$\}$?

1.7 CONSTRUCCIÓN DE UN LENGUAJE

Hemos visto ya la necesidad, si se quiere hacer la teoría de conjuntos con una buena dosis de rigor, de construir un lenguaje que nos permita expresar con exactitud los hechos de tal teoría. En la sección primera introdujimos los conectivos proposicionales y desarrollamos en parte el cálculo proposicional, el cual puede considerarse como una primera tentativa de construcción de un lenguaje; sin embargo rápidamente se observa que es insuficiente para la mayoría de nuestros propósitos; por ejemplo, expresiones como

(1) "El cuadrado de todo número real es mayor que o igual a cero", o,
(2) "No existe un número real mayor que todos los naturales",

tan sólo podrían representarse por p y $\neg q$ respectivamente; si designamos la proposición "$1^2 \geq 0$" por r, la implicación "$p \to r$" no sería una tautología (ya que los valores de verdad de r nada tienen que ver con los de p), es decir, que de "El cuadrado de todo número real es mayor que o igual a cero", no podríamos deducir que "$1^2 \geq 0$".

Según lo visto en la sección 2, tomando a $\mathbb{R}$ como referencial, sería más correcto representar (1) y (2) respectivamente por

$$(\forall x)(x^2 \geq 0) \qquad y$$
$$\neg(\exists x)(\forall n \in \mathbb{N})(x > n).$$

Análogamente, las leyes conmutativa e invertiva de la adición se expresarían por

$$(\forall x)(\forall y)(x + y = y + x) \qquad \text{y}$$
$$(\forall x)(\exists y)(x + y = 0).$$

Se hace entonces imprescindible en el lenguaje la presencia de los cuantificadores, de las variables, de símbolos constantes en algunos casos (el cero, p. ej.), de expresiones como "es triángulo isóceles", "es menor que" ("$<$"), "$x + y = 0$", "$x^2 + y^2 = z^2$", "$X \in Y$", etc.

Aparecen en el lenguaje dos clases de expresiones: las que describen objetos (que se llamarán los *términos*) y las que *expresan* las relaciones entre los objetos (las *fórmulas bien formadas*).

Expresiones como $x^2 + y^2$, $x + y$, $x \cdot y$, 0, $5 + 8, x$, etc. se llaman *términos*. Intuitivamente, nombran o describen objetos, o se transforman en nombres o descripciones de objetos al reemplazar las variables por nombres

o descripciones. Por ejemplo, si en $x+y$ reemplazamos x por 3 y y por 5, se obtiene 3+5 que es un nombre del número ocho; los sustantivos, nombres y pronombres entre otros, serían términos del idioma usual.

Expresiones como "T es triángulo isóceles", "x es un hombre", "x es padre de y", "$x < y$" y "$a \in b$", se llaman *predicados* (de una variable los dos primeros y de dos variables o "argumentos" los tres últimos). Sirven para hacer afirmaciones acerca de los objetos o para establecer relaciones entre objetos.

Observamos también la presencia de operaciones como + y · entre números reales; éstas son en esencia funciones (por ejemplo + es una función de $\mathbb{R}^2$ en $\mathbb{R}$: $+(x,y) = x+y$). Una operación enearia en $\mathbb{R}$ es una función $f : \mathbb{R}^n \to \mathbb{R}$.

En general, en un lenguaje llamado de primer orden, construido para expresar los hechos de una teoría matemática, intervienen los símbolos siguientes, organizados (según [1]) en dos clases: *los lógicos*, que se usan en todas las teorías y siempre con los mismos significados y *los específicos o parámetros*, es decir, aquellos símbolos propios de cada lenguaje particular y que son susceptibles de ser interpretados, o sea que en diferentes estructuras pueden poseer distintos significados.

Símbolos lógicos.

Ellos son:

a) Los paréntesis (,) y serán los únicos símbolos de agrupación que se usarán.

b) Los conectivos proposicionales $\neg$, $\to$, $\vee$, $\wedge$, $\leftrightarrow$.

c) Las variables. Es suficiente tener tantas como números naturales: $x, y, z, x_1, x_2, x_3, \ldots$.

d) El símbolo de igualdad. Es tan sólo opcional, ya que algunas teorías no lo usan o lo pueden introducir posteriormente como un símbolo definido.

e) El cuantificador universal $\forall$ (y ya que $(\exists x)p(x)$ se puede expresar como $\neg(\forall x)(\neg p(x))$, también usaremos el cuantificador existencial $\exists$).

Símbolos específicos o parámetros.

Ellos comprenden:

a) Los símbolos constantes: aquellos que representan objetos específicos, fijos, del universo, los mismos todo el tiempo. El conjunto de los símbolos constantes puede ser vacío ya que hay teorías que no los requieren inicialmente.

b) Los símbolos predicales o relacionales: son los símbolos para designar predicados o relaciones. Para cada entero positivo n puede haber un conjunto de tales símbolos, llamados símbolos predicales de n argumentos y se usan para designar relaciones enearias.

c) Los símbolos funcionales o de operación (son los símbolos para designar operaciones unitarias, binarias, ternarias, etc). Para cada entero positivo n puede existir un conjunto de tales símbolos, llamados símbolos funcionales de n argumentos o de operaciones enearias.

Por ejemplo, en un lenguaje para estudiar los números reales, se incluyen todos los símbolos lógicos y entre los específicos se tienen los símbolos constantes 0 y 1, y únicamente un símbolo predical, el "<" , de dos argumentos; los símbolos funcionales "+", "·", también de dos argumentos, para la adición y la multiplicación respectivamente.

Los términos se definen en la forma siguiente: Las variables y los símbolos constantes son términos; los demás se generan a partir de los anteriores mediante los símbolos funcionales: si f es un símbolo funcional de ene argumentos y $t_1, t_2, \ldots, t_n$ son términos, $f(t_1, t_2, \ldots, t_n)$ es un término. Intuitivamente, f es un símbolo que representa una operación enearia y $f(t_1, t_2, \ldots, t_n)$ es el símbolo que representa el resultado de efectuar dicha operación entre los términos $t_1, t_2, \ldots, t_n$. Por ejemplo, en un lenguaje para los números reales, +(1,1) es una expresión que en $\mathbb{R}$ se debe interpretar como 1+1.

Sabiendo cuales son las expresiones que describen objetos, surge el problema de dar las reglas sintácticas para formar las expresiones que describen propiedades de los objetos o relaciones entre objetos, es decir para formar las expresiones con sentido o *fórmulas bien formadas (f.b.f.)* del lenguaje. Cuando se tienen predicados como "es un positivo", "<", "... es menor que ... y que ... ", de uno, dos y tres argumentos respectivamente, entonces al aplicarlos a conjuntos adecuados de términos, se obtienen las expresiones con sentido más simples que pueden formarse, llamadas las *fórmulas atómicas*. Por ejemplo, "1 es un positivo", "$x \cdot x + y \cdot y$ es un positivo", "$0 < (1+1)(((1+1)+1)+1)$", "$1 < 0$", "$x < x \cdot x + 1$", "$(1+1) \cdot (1+1)$ es mayor que 1+1 y que 1", "x es mayor que 0 y que 1", etc., son fórmulas atómicas de un lenguaje para los números reales. También lo son "$1+1 = x$" y "$x \cdot (y+1) = (1+1) \cdot 1$".

Formalizando un poco:

Si R es un símbolo predical de ene argumentos y $t_1, t_2, ..., t_n$ son términos, entonces $R(t_1, t_2, \ldots, t_n)$ es una fórmula atómica (intuitivamente R es un símbolo que representa un predicado y $R(t_1, t_2, \ldots, t_n)$ es una expresión que representa la aplicación del predicado R a los objetos representados por $t_1, t_2, ..., t_n$).

Además, si en el lenguaje se incluye la igualdad y t_1, t_2 son términos, entonces $t_1 = t_2$ también es una fórmula atómica.

Proseguimos de manera análoga al caso del cálculo proposicional:

1) Las fórmulas atómicas son f.b.f.

2) Si α es una f.b.f., también lo es $(\neg\alpha)$.

3) Si α, β son f.b.f. también lo son $(\alpha \to \beta)$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$ y $(\alpha \leftrightarrow \beta)$.

4) Si α es una f.b.f. y x es una variable, entonces $(\forall x)\alpha$ es una f.b.f. (y según lo dicho antes también lo es $(\exists x)\alpha$).

5) Una expresión es una f.b.f. si y sólo si puede obtenerse aplicando las cuatro reglas anteriores finitas veces.

Por ejemplo, en un lenguaje para los números reales son f.b.f. las siguientes:

$$(\forall x_1)(\exists x_2)((x_1 + x_2 = 0) \vee (x_2 + x_1 = 0)).$$

$$\neg(\exists x_2)(\forall x_1)(x_1 < x_2),$$

$$((x_1 < x_2) \wedge (x_2 < x_1)) \vee (\neg(x_1 \cdot x_3 = 1)).$$

No lo son:

$$x_1 \to \neg(\forall x_2), \qquad x_1 \to x_2\ ,$$
$$(\exists x_2) > x_1, \quad (\neg(x_1 + x_2) \to (x_1 < x_2))\ ,$$
$$(x_1 \neq x_2) \wedge (x_3 \neq x_1 \wedge x_3 \neq x_2) \wedge (x_4 \neq x_1 \wedge x_4 \neq x_2 \wedge x_4 \neq x_3) \wedge \ldots$$

(la última por aplicar infinitas veces las reglas 2) y 3)).

Los ejemplos que hemos dado se han centrado en un lenguaje para los números reales; regresando a nuestro tema, construyamos ahora un lenguaje para desarrollar la teoría de conjuntos. En él incluiremos todos los símbolos lógicos, inclusive la igualdad y solamente un único símbolo predical de dos argumentos, "$\in$", para la pertenencia.

Lo anterior significa que realmente los únicos conceptos que tomamos como primitivos son el de igualdad y el de pertenencia; todos los demás, incluyendo los de las operaciones entre conjuntos, podrán definirse mediante los primitivos.

A primera vista puede parecer un lenguaje muy pobre, pero es casi suficiente para expresar cuanto queramos decir sobre los conjuntos; además, entre más sencillo sea, más precisas se hacen las reglas que lo gobiernan y menos equivocaciones se cometen (o mejor menos tonterías se dicen).

Inicialmente las únicas fórmulas atómicas que aparecen son las de la forma $X \in Y$ y $X = Y$, donde X, Y son variables; posteriormente, definidas las operaciones de unión, intersección, diferencia, etc., aparecerán otras como $(X \in (Y \cup Z)$, $X \in (Y \cap Z)$, $(Y - Z) \in X$ y $X = Y \cup Z$; luego, introduciendo el conjunto vacío $\emptyset$ y la relación binaria de contenencia $(\subseteq)$, también se tendrán $\emptyset \in X, \emptyset \in X \cup Y$, $\emptyset = X \cap Y, \emptyset \subseteq X$, $X \subseteq Y$, etc.

Nota: Seguiremos la costumbre de usar además de (o en vez de) las variables $x_1, x_2, \ldots$, letras del alfabeto como a, b, x, A, B, X, Y, Z, etc.

Ejercicios

1. En el lenguaje para la teoría de conjuntos acabado de describir, y según los conocimientos adquiridos sobre conjuntos, diga cuáles de las expresiones siguientes son f.b.f. y cúales no.

   (a) $x \in (A \vee B)$.
   (b) $x \in A \vee x \in B$.
   (c) $(x \in A \vee x \in B) = (x \in B \vee x \in A)$.
   (d) $A \in \emptyset$.
   (e) $(\forall X)(X \in X)$.
   (f) $(\forall Y)(X \in X)$.
   (g) $(x \in A \cup B) = (x \in A \vee x \in B)$.
   (h) $A \cup B = (x \in A \vee x \in B)$.
   (i) $A - B = A \cap (S - B)$.
   (j) $(x \in A \cup B) \to (x \in A \vee x \in B)$.
   (k) $(x \in A - B) \leftrightarrow (x \in A \to x \in B)$.
   (l) $Y \subseteq Y \leftrightarrow (Y \in Y)$.

(m) $\neg(A \cup B) = ((\neg A) \vee (\neg B))$.

(n) $A \cap B = A \cap (A \cup B)$.

(o) $(x \in A \cap B) \leftrightarrow (x \in A \vee x \in B)$.

(p) $(x \in A \cap B) \leftrightarrow (x \in A \wedge x \in B)$.

(q) $A - B = (x \in A \wedge x \notin B)$.

(r) $(x \in A - B) \rightarrow (x \in A \rightarrow x \notin B)$.

(s) $(\bigcup_{A \in \mathfrak{C}} A) = (\exists A \in \mathfrak{C})(x \in A)$.

(t) $(x \in \bigcup_{A \in \mathfrak{C}} A) \leftrightarrow (\forall A \in \mathfrak{C})(x \in A)$.

2. Usando exclusivamente el lenguaje de la teoría de conjuntos propuesto, defina los símbolos funcionales "$\cup$" e "$\cap$" de dos argumentos y el símbolo relacional binario "$\subseteq$".

3. En el lenguaje de la teoría de conjuntos, incluyendo los símbolos definidos en el ejercicio 2) y el símbolo $\emptyset$ para designar al conjunto vacío, escribir las afirmaciones siguientes:

   (a) El conjunto A es subconjunto propio de los conjuntos B y C.

   (b) Ningún conjunto es elemento de sí mismo.

   (c) Vacío es subconjunto de todo conjunto.

   (d) Dos conjuntos son iguales si y sólo si tienen los mismos elementos.

   (e) La intersección de dos conjuntos es subconjunto de cada uno de los conjuntos que se intersectan.

   (f) No existen dos conjuntos tales que cada uno de ellos sea elemento del otro.

   (g) No existe un conjunto al cual pertenezcan todos los conjuntos.

   (h) Dados dos conjuntos cualesquiera, siempre existe otro del cual los dos son subconjuntos.

   (i) Dados dos conjuntos cualesquiera, existe otro al cual pertenecen como elementos los conjuntos dados.

   (j) Dado cualquier conjunto, siempre existe otro no vacío que no posee elementos en común con el primero.

4. Traduzca al español correcto, las expresiones siguientes, escritas en el lenguaje de la teoría de conjuntos.

   (a) $\neg(\forall X)(X \in X)$

   (b) $(\forall X)(\neg(X \in X))$

   (c) $(\forall X)(\exists Y)(Y \notin X)$

   (d) $(\exists X)(\forall Y)(\neg(Y \in X))$

   (e) $(\forall A)(\forall B)(\exists C)(\forall Z)(Z \in C \leftrightarrow (Z \in A \wedge \neg(Z \in B)))$.

5. Supongamos que para hablar de números naturales se construye un lenguaje incluyendo todos los símbolos lógicos y los siguientes parámetros: el símbolo predical de dos argumentos "$<$", los símbolos funcionales de dos argumentos "$+$" y "$\cdot$" y los símbolos constantes "0" y "1".

   a) Dé cinco ejemplos de f.b.f. de dicho lenguaje.

   b) Exprese en este lenguaje:

      i. No existe un natural mayor que todos los naturales.

      ii. Existe un natural menor que todos los naturales.

      iii. La multiplicación de naturales es modulativa.

      iv. La multiplicación de naturales es distributiva con respecto a la adición.

   c) ¿Podría definirse en este lenguaje el símbolo predical "p" de un argumento para expresar "es primo"?

**

Capítulo 2

DESARROLLO AXIOMÁTICO

2.1 PRIMEROS AXIOMAS

Una vez que aparecieron en el seno de la teoría intuitiva de conjuntos las primeras paradojas, los matemáticos convencidos de la naturalidad y utilidad de tal teoría y de su poder unificador dentro de la matemática, en vez de desecharla trataron de rehacerla, de perfeccionarla, presentándola como una ciencia deductiva.

Surgió entonces la pregunta siguiente: ¿Cuáles deben ser las proposiciones que deben tomarse como axiomas de tal manera que se eliminen las paradojas (que la teoría sea consistente) y que a partir de dichos axiomas puedan deducirse como teoremas la mayor cantidad posible de aquellas proposiciones conocidas ya como ciertas en la teoría intuitiva?

Se propusieron varias respuestas; algunas de ellas fueron dejadas de lado por su inconveniencia, su complejidad o porque más tarde se dedujo alguna contradicción en ellas; otras fueron acogidas y perfeccionadas posteriormente por otros matemáticos. Se puede afirmar que la axiomatización de la teoría de conjuntos ha sido uno de los logros más notables da la matemática en el siglo XX. Vale la pena hacer referencia a tres de ellas.

(a) "*La teoría de tipos*" propuesta por Russell y Whitehead en su famoso libro "*Principia Mathematica*", por los años de 1910 - 1913. Debido a su complejidad es poco usada hoy en día.

(b) *El sistema axiomático de Zermelo-Frankel.* Fue propuesto por E. Zermelo en 1908 y debido a su inconveniencia para tratar la aritmética ordinal y la inducción transfinita, fue modificada en 1922 independientemente por A. Fraenkel y T. Slokem, eliminando la anterior dificultad con la introduc-

ción del esquema axiomático de sustitución. Es el tratamiento maś cercano a la teoría intuitiva y el que desarrollaremos en el presente libro.

(c) "*La teoría de clases*" propuesta originalmente por J. Von Neumann y modificada por P. Bernays y K. Gödel. Sus diferencias con el sistema de Zermelo-Fraenkel pueden ponerse de presente tomando un texto como [6] o [7] y comparándolo con las presentes notas. Dichas diferencias radican esencialmente en que como concepto primitivo se toma el de clase (todo conjunto es una clase pero existen clases -como la de todos los conjuntos- que no son conjuntos) y en que es posible caracterizarlo mediante un conjunto finito de axiomas, es decir, todos ellos redactados en el lenguaje objeto de la teoría. Esto no ocurre en la teoría de Zermelo-Fraenkel (ver el axioma A3 más adelante).

Ya situados, comencemos el estudio de la teoría axiomática de conjuntos.

Como lo dijimos en la sección 5 del capítulo anterior, nuestros conceptos primitivos son el de *conjunto* y el de *pertenencia*; por este motivo, siempre estaremos hablando de ellos, es decir, supondremos que en el universo del discurso tan solo habrá conjuntos y nada más; unos conjuntos podrán pertenecer a otros en cuyo caso se dirá que los primeros son *elementos* de los segundos. En el tratamiento intuitivo hemos considerado conjuntos como

$$\{\text{Luis, Juan}\} \text{ o } \{\text{Bogotá, } a, b, 1.2, \text{ hierro}\}$$

con elementos de los cuales se podría pensar que no son conjuntos sino otro tipo de entes a los cuales se les podría llamar *individuos* ó *átomos*.

Existen desarrollos axiomáticos (ver [8] ó [9]) donde se poseen individuos y conjuntos, pero como lo dijimos antes, tan solo consideraremos conjuntos para mayor simplicidad y debido a que la teoría así constituida es también suficiente para todos los fines de la matemática.

El primer axioma tiene por objeto formalizar nuestro conocido criterio para decidir cuándo se tiene la igualdad entre conjuntos.

A1 - Axioma de extensión.

$$(\forall X)(\forall Y)((\forall Z)(Z \in X \leftrightarrow Z \in Y) \rightarrow X = Y)$$

En español sería: Cualesquiera sean los conjuntos X, Y, si todo elemento de X es elemento de Y y todo elemento de Y es elemento de X, entonces X es igual a Y.

Un axioma lógico de la igualdad dice que si $X = Y$, entonces toda propiedad poseída por X también es poseída por Y, y recíprocamente. En particular

si $X = Y$, entonces $Z \in X \leftrightarrow Z \in Y$ cualquiera sea Z, es decir,

$$(\forall X)(\forall Y)(X = Y \rightarrow (\forall Z)(Z \in X \leftrightarrow Z \in Y)).$$

Esta fórmula junto con A1 producen

$$(\forall X)(\forall Y)(X = Y \leftrightarrow (\forall Z)(Z \in X \leftrightarrow Z \in Y)),$$

es decir, que "*dos conjuntos son iguales si y sólo si poseen los mismos elementos*", la cual es una manera muy común de enunciar el axioma de extensión, precisamente la forma como fué presentado en el tratamiento intuitivo.

DEFINICIÓN 1. Diremos que X es un subconjunto de $Y (X \subseteq Y)$ si todo elemento de X es también elemento de Y. En el lenguaje de la teoría: $X \subseteq Y \leftrightarrow (\forall Z)(Z \in X \rightarrow Z \in Y)$.

Si $X \subseteq Y$ y además $X \neq Y$ $(\neg(X = Y))$, diremos que X es un subconjunto propio de Y y lo notaremos $X \subset Y$.

Nuestro primer teorema podría ser entonces el siguiente:

TEOREMA 1. Dos conjuntos son iguales si y sólo cada uno de ellos es subconjunto del otro es decir, $(\forall X)(\forall Y)(X = Y \leftrightarrow X \subseteq Y \wedge Y \subseteq X))$.

Este teorema es inmediato de la definición anterior y de la última forma de enunciar el axioma de extensión.

El conjunto más simple que consideraremos es el conjunto vacío y nuestro próximo axioma es exactamente su presentación en sociedad:

A2 - Axioma del conjunto vacío.

$$(\exists Y)(\forall X)(\neg(X \in Y)).$$

Es decir, existe un conjunto sin elementos. Combinándolo con A1 obtenemos que dicho conjunto sin elementos es único, ya que si existiesen Y, Z con esta propiedad, se tendría $X \in Y \leftrightarrow X \in Z$ (los dos miembros de la equivalencia son falsos, cualquiera sea X) y A1 implicaría $Y = Z$. Para designar a este único conjunto sin elementos usaremos el símbolo constante $\emptyset$, como es la costumbre.

Antes de enunciar el siguiente axioma, tenemos necesidad de introducir algunos conceptos lógicos más. Situémonos dentro de un lenguaje de primer orden; tomemos una de sus f.b.f. que posea al menos un cuantificador

y consideremos uno de sus cuantificadores; por *alcance* de este cuantificador (en la f.b.f. dada) entendemos la f.b.f. constituida por el cuantificador mismo junto con la variable que 'usa' y la f.b.f. a la cual se está aplicando dicho cuantificador (esta última es la f.b.f. de menor longitud que sigue inmediatamente al cuantificador).
Por ejemplo en $(\forall X)(\forall Y)((\forall Z)(Z \in X \leftrightarrow Z \in Y) \rightarrow X = Y)$ el alcance del primer cuantificador es la fórmula completa, el del segundo es $(\forall Y)((\forall Z)(Z \in X \leftrightarrow Z \in Y) \rightarrow X = Y)$ y el del tercer cuantificador es $(\forall Z)(Z \in X \leftrightarrow Z \in Y)$. En $(\forall X)(X = \emptyset \vee (\exists Y)(Y \in X))$ el alcance de "$\forall$" es la fórmula completa y el de "$\exists$" es $(\exists Y)(Y \in X)$. En $(\forall X)(X \neq \emptyset \rightarrow (\exists Y)(Y \cap X = \emptyset))$ el alcance de "$\forall$" también es la fórmula completa y el de "$\exists$" es $(\exists Y)(Y \cap X = \emptyset)$.

Si en una f.b.f. la ocurrencia de una variable se halla dentro del alcance de un cuantificador que 'use' dicha variable, se dice que dicha ocurrencia es *ligada*. En caso contrario, se dice que la ocurrencia es *libre*; Por ejemplo, en $(\forall X)(X^2 + Y^2 < 2)$ todas las ocurrencias de X son ligadas y la de Y es libre: en $(\forall X)(X + Y = Y + X) \wedge Y = X + 3$, la última ocurrencia de X (en $Y = X + 3$) es libre y todas las demás son ligadas; además aquí todas las ocurrencias de Y son libres.

Una f.b.f. se llamará una *proposición* si en ella todas las ocurrencias de sus variables son ligadas. Por ejemplo, $(\forall X)(X \notin \emptyset)$ lo es, lo mismo que $(\forall X)(\exists Y)(\forall Z)(Z \in Y \leftrightarrow Z \subseteq X)$.

Una variable es libre en una f.b.f. si al menos una de sus ocurrencias (en la f.b.f. dada) es libre; *una proposición viene a ser entonces una f.b.f. sin variables libres.*

Nos encontramos ahora en posición de continuar con el estudio de los conjuntos; nos proponemos corregir en lo posible los defectos que presentaba la determinación de conjuntos por comprensión.

El primer paso en esta dirección consiste en definir con precisión el concepto de "condición": *Una condición* en X es una f.b.f. en la cual la variable X es libre; por ejemplo $X^2 - 1 = 0$, $(\exists Y)(X^2 + Y^2 < 1)$, $X \in A \vee X \in B$, etc. son condiciones en X.

Una f.b.f. en la cual existe una variable X con al menos una ocurrencia de X libre, es una *condición en* X, y no una proposición. Por ejemplo, $X > 1 \wedge (\forall Y)(\forall Z)(X = YZ \rightarrow (Y = 1 \vee Z = 1))$ no es una proposición sino una condición en X.

El segundo paso se da determinando cúales son las condiciones que podemos usar para definir conjuntos: Sólo podremos emplear en la definición de conjuntos por comprensión aquellas condiciones que sean f.b.f. del lenguaje objeto que hemos construido previamente para desarrollar la teoría de conjuntos. Ya no se podrán entonces formar conjuntos como el de los objetos abstractos puesto que "X es un objeto abstracto" no es una de las condiciones aceptadas; sin embargo $\neg(X \in X)$ sí lo es y se podría formar aún el conjunto $B = \{X \mid \neg(X \in X)\}$ de la paradoja de Rusell; ¿Qué hacer entonces? Zermelo afirmó que para determinar un conjunto no bastaba con dar la propiedad que debían cumplir sus elementos, sino que era necesario dar además un conjunto (el referencial) a cuyos elementos aplicar la propiedad, formándose así un nuevo conjunto constituido por aquellos elementos del referencial que cumplen la condición dada. Podemos resumir el párrafo anterior en la forma siguiente:

A3 - Esquema axiomático de separación.

"A todo conjunto A y a toda condición $\varphi(X)$ corresponde un conjunto B cuyos elementos son precisamente aquellos elementos X de A para los cuales se cumple $\varphi(X)$".

El conjunto B se forma "*separando*" de A aquellos elementos que satisfacen φ.

El nombre de "esquema axiomático" se debe a que no es propiamente un axioma (no es una f.b.f. del lenguaje objeto de la teoría) sino que está redactado en términos del metalenguaje y es en realidad un molde para producir axiomas, ya que a cada condición corresponde un axioma, y existen infinitas condiciones, en verdad tantas como números naturales (?).

El esquema axiomático A3 se aplica generalmente cuando $\varphi(X)$ es una condición con X como única variable libre, pero no es estrictamente necesario; puede ser una f.b.f. con más de una variable libre; por ejemplo, si la condición es $X \in \{\{1,2\}, \{2,3,4\}\} \wedge X \subseteq Y$, entonces para todo valor específico que se dé a Y y para todo A, se determina un conjunto B. (Si $Y = \{2,3,4,5,6\}$ y $A = \{\{1\}, \{2,3,4\}, \{5,6\}\}$), se obtiene $B = \{\{2,3,4\}\}$.

Se puede formular un enunciado más "preciso" de A3:

A3′ - Esquema axiomático de separación.

Cualquier f.b.f. de la forma

$$(\forall Y_1)(\forall Y_2)...(\forall Y_n)(\forall A)(\exists B)((\forall Z)(Z \in B \leftrightarrow Z \in A \wedge \varphi(Z; Y_1, Y_2, ..., Y_n))$$

es un axioma, siempre que $\varphi(Z; Y_1, Y_2, ..., Y_n)$ sea una f.b.f. del lenguaje objeto de la teoría de conjuntos con al menos una variable libre (Z) y con

Z, $Y_1, Y_2, ..., Y_n$ como únicas variables libres de φ, con A y B variables distintas, con B distinta de Z y de $Y_1, Y_2, ..., Y_n$.

Las restricciones impuestas pueden justificarse con casos como los siguientes:
Si pudiesen ser A y B la misma variable podríamos obtener
$(\forall Z)(Z \in A \leftrightarrow Z \in A \wedge Z \neq Z)$; reemplazando A por $\{\emptyset\}$ se tendrá
$(\forall Z)(Z \in \{\emptyset\} \leftrightarrow Z \in \{\emptyset\} \wedge Z \neq Z)$, de donde
$(\forall Z)(Z = \emptyset \leftrightarrow Z = \emptyset \wedge Z \neq Z)$ y en particular para $Z = \emptyset$, se obtiene la contradicción $\emptyset = \emptyset \leftrightarrow (\emptyset = \emptyset \wedge \emptyset \neq \emptyset)$.

Si B fuese una de las variables libres de φ, se podría tener $(\forall A)(\exists B)$ $(\forall Z)(Z \in B \leftrightarrow Z \in A \wedge Z \notin B)$, con $Z \notin B$ como φ. Para $A = \{\emptyset\}$ existiría B tal que $(\forall Z)(Z \in B \leftrightarrow Z \in \{\emptyset\} \wedge Z \in B)$. Si en particular tomamos $Z = \emptyset$, $\emptyset \in B \leftrightarrow \emptyset \in \{\emptyset\} \wedge \emptyset \notin B$.

Siendo verdadero $\emptyset \in \{\emptyset\}$, se deduce $\emptyset \in B \leftrightarrow \emptyset \notin B$, lo cual es una contradicción.

Si combinamos A3′ con A1, obtenemos:

TEOREMA 2 (Esquema). *El conjunto B cuya existencia se afirma en el esquema axiomático de separación, es único.*

En efecto, ya que si existiese otro conjunto B' que cumpliese las condiciones de A3′, se tendría

$$[(\forall A)(\exists B)(\forall Z)(Z \in B \leftrightarrow Z \in A \wedge \varphi(Z))] \wedge [(\forall A)(\exists B')(\forall Z)(Z \in B' \leftrightarrow Z \in A \wedge \varphi(Z))]$$

de donde $(\forall Z)((Z \in B \leftrightarrow Z \in A \wedge \varphi(Z))(Z \in B' \leftrightarrow Z \in A \wedge \varphi(Z)))$ y por transitividad de la equivalencia, $(\forall Z)((Z \in B \leftrightarrow Z \in B')$, lo cual después de A1 significa que $B = B'$.

Nota. En realidad, el anterior, más que un teorema, es un esquema, un molde que produce tantos teoremas como A3. El Teorema 2 justifica la siguiente notación usual para el conjunto $B : \{Z \in A \mid \varphi(Z)\}$, es decir,

$$Z \in \{Z \in A \mid \varphi(Z)\} \leftrightarrow Z \in A \wedge \varphi(Z). \qquad (*)$$

Utilizando los axiomas y teoremas vistos hasta el momento, podemos legitimar las definiciones dadas en el desarrollo intuitivo que introdujeron subconjuntos de conjuntos dados. Por ejemplo, la diferencia entre conjuntos

$$A - B = \{Z \in A : Z \notin B\}$$

es el único conjunto obtenido separando de A los elementos Z que cumplen la condición $Z \notin B$.

La intersección de dos conjuntos se forma separando del primero aquellos elementos que pertenecen al segundo:

$$A \cap B = \{Z \in A : Z \in B\}.$$

La intersección de los conjuntos de una colección $\mathfrak{C}$ se forma tomando uno de los conjuntos de $\mathfrak{C}$ y separando de él aquellos elementos que pertenecen a todos los conjuntos de $\mathfrak{C}$; por ese motivo $\mathfrak{C}$ no puede ser vacía, una salvedad que no habíamos hecho en el desarrollo intuitivo.

En el lenguaje objeto: Si $A \in \mathfrak{C}$,

$$\cap\mathfrak{C} = \{Z \in A \mid (\forall V)(V \in \mathfrak{C} \rightarrow Z \in V)\}$$

A primera vista puede parecer que $\cap\mathfrak{C}$ depende del conjunto A, pero esto no es así: Es evidente que

$$(Z \in A \ \wedge \ (\forall V)(V \in \mathfrak{C} \rightarrow Z \in V)) \rightarrow ((\forall V)(V \in \mathfrak{C} \rightarrow Z \in V)$$

Recíprocamente: sabemos que

(1) $A \in \mathfrak{C}$. Si

(2) $(\forall V)(V \in \mathfrak{C} \rightarrow Z \in V)$, en particular se tiene que

(3) $A \in \mathfrak{C} \rightarrow Z \in A$ y por Modus Ponens, de (1) y (3),

(4) $Z \in A$. Luego, de (2) y (4),

(5) $Z \in A \ \wedge \ (\forall V)(V \in \mathfrak{C} \rightarrow Z \in V)$.

El paso de (2) a (5) significa que bajo la hipótesis $A \in \mathfrak{C}$ se tiene que $(\forall V)(V \in \mathfrak{C} \rightarrow Z \in V) \rightarrow (Z \in A \ \wedge \ (\forall V)(V \in \mathfrak{C} \rightarrow Z \in V))$.

En resumen, bajo la hipótesis $A \in \mathfrak{C}$ se cumple que

$$(Z \in A \ \wedge \ (\forall V)(V \in \mathfrak{C} \rightarrow Z \in V)) \leftrightarrow (\forall V)(V \in \mathfrak{C} \rightarrow Z \in V)$$

es decir $Z \in \cap\mathfrak{C} \leftrightarrow (\forall V)(V \in \mathfrak{C} \rightarrow Z \in V)$, no dependiendo de A y bastando con que $\mathfrak{C}$ sea no vacío.

Mostremos ahora que con los axiomas introducidos ya se elimina de la teoría la paradoja de Russell:

Después del axioma de separación, *no* nos está permitido formar el conjunto $B = \{X \mid X \notin X\}$, sino que la condición $X \notin X$ debe usarse para

separar de un conjunto aquellos elementos que la cumplen; sea A ***cualquier*** conjunto; sea $B = \{X \in A \mid X \notin X\}$. Según $(*)$,

$$(\forall X)(X \in B \leftrightarrow X \in A \ \wedge \ X \notin X)$$

Si $X = B$, se tiene

$$(B \in B \leftrightarrow B \in A \ \wedge \ B \notin B) \qquad (\#)$$

¿Puede ser cierto $B \in B$? NO, porque entonces $B \in A \ \wedge \ B \notin B$, también sería cierto; en particular $B \notin B$, lo cual sería contradictorio con la suposición $B \in B$.

Debe cumplirse entonces $B \notin B$, en cuyo caso deberá ser falso $B \in B$ y para que se cumpla la equivalencia $(\#)$ sin incurrir en contradicciones hay una única forma, que $B \in A$ sea falso:

$$\underbrace{\underbrace{B \in B}_{\text{F}} \longleftrightarrow \underbrace{\underbrace{B \in A}_{\text{F}} \wedge \underbrace{B \notin B}_{\text{V}}}_{\text{F}}}_{\text{V}}$$

Hemos eliminado así la paradoja de Russell y de paso hemos demostrado dos cosas:
(a) $B \notin B$
(b) $B \notin A$, es decir,

$$(\forall A)(\{X \in A \mid X \notin X\} \notin A)$$

o sea que cualquiera sea A, existe al menos un conjunto que no pertenece a A; en el lenguaje objeto de la teoría de conjuntos, $\forall A \exists B(B \notin A)$, o equivalentemente, $\neg(\exists A)(\forall B)(B \in A)$); en otras palabras:

TEOREMA 3. *No existe un conjunto al cual pertenezcan todos los conjuntos; o más brevemente, no existe el conjunto de todos los conjuntos.*

Hemos matado así dos pájaros de un solo tiro, ya que de paso hemos eliminado también las paradojas (como la del mayor cardinal, sección 6, Cap.I) que se originaban en el supuesto de la existencia del conjunto de todos los conjuntos.

Ejercicios

1. En las fórmulas que siguen, halle el alcance de cada uno de los cuantificadores que aparecen:

   (a) $(\forall Y)(X \cup Y = Y \cup X)$.
   (b) $(\forall X)(X \cup \emptyset = X) \wedge (X \supseteq \emptyset)$.
   (c) $(\forall X)((X \cup \emptyset = X) \wedge (X \supseteq \emptyset))$.
   (d) $(\exists Y)(Y \in \mathfrak{A} \ \wedge \ X \in Y)$.
   (e) $(\forall A)(\exists X)(X \in A \ \wedge \ (\forall Z)(Z \in X \rightarrow Z \notin A))$.
   (f) $\neg(\exists X)(\exists Y)(X \in Y \ \wedge \ Y \in X)$.
   (g) $(\exists X)(\forall A)(X \cup A = X)$.
   (h) $X \neq \emptyset \rightarrow (\exists Y)(Y \in X)$.
   (i) $\neg(\exists Y)(Y \supseteq A)$.
   (j) $(\forall A)(A \neq \{A\})$.

2. En cada una de las f.b.f. del ejercicio anterior, diga de las variables que aparecen, cuáles ocurrencias son ligadas y cuáles libres; diga además cuáles f.b.f. son proposiciones y de éstas cuáles son verdaderas (apoyándose más que todo en su intuición).

3. Coloque adecuadamente uno o varios cuantificadores, según el caso, en cada una de las f.b.f. del ejercicio 1. que posean variables libres. de tal manera que se transformen en proposiciones, ojalá verdaderas si es posible.

4. Sea E un conjunto dado; ¿qué conjuntos se obtienen al aplicar a E el axioma de separación tomando como $\varphi(X)$:

   (a) $X = X$,
   (b) $X \neq X$,
   (c) $X \notin X$,
   (d) $(\forall A)(A \in \emptyset \rightarrow X \in A)$,
   (e) $A \subseteq E \ \wedge \ X \notin A$.?

5. Supongamos que en vez de A2 damos como axioma "Existe al menos un conjunto". Aplique a este conjunto A el axioma de separación con

la condición $X \neq X$; llame al conjunto obtenido $\emptyset_A$. Pruebe que si $\emptyset_B = \{X \in B | X \neq X\}$ para otro conjunto B, entonces $\emptyset_A = \emptyset_B$.

Siendo único el conjunto obtenido al aplicar $X \neq X$ a cualquier conjunto, llámelo $\mathbb{C}$ y demuestre que $(\forall X)(X \notin \emptyset)$. Una pregunta: ¿Podría escribir "Existe al menos un conjunto" en el lenguaje objeto que hemos dado para la teoría de conjuntos?

6. Dé un ejemplo de un conjunto A cuyos elementos sean a la vez subconjuntos de A.

7. (a) Si $\mathfrak{C}$ es la colección vacía, demuestre (por el absurdo) que $\cap\mathfrak{C}$ o sea $\{x \mid (\forall A)(A \in \mathfrak{C} \rightarrow x \in A)\}$, no existe. Ayuda: Si existiese, sería el conjunto de todos los conjuntos.

   (b) Si M es un conjunto cualquiera, al conjunto

$$\{x \in M : (\forall A)(A \in \emptyset \rightarrow x \in A)\}.$$

   Se le llama "la intersección de la colección vacía de subconjuntos de M". ¿A qué es igual dicha intersección?

2.2 REUNIONES Y CONJUNTOS DE PARTES

Hasta este momento el único conjunto que conocemos "oficialmente" es el conjunto vacío y como el esquema axiomático de separación sólo nos permite construir subconjuntos de conjuntos dados previamente y el único subconjunto de $\emptyset$ es el mismo $\emptyset$, necesitamos nuevos axiomas para formar conjuntos que no sean vacíos, conjuntos "más grandes" o de naturaleza un tanto diferente a los dados.

A4 - **Axioma del conjunto binario.**

Dados dos conjuntos cualesquiera, existe otro conjunto cuyos elementos son precisamente los dos conjuntos dados.

En el lenguaje objeto:

$$(\forall A)(\forall B)(\exists C)(\forall Z)[Z \in C \leftrightarrow (Z = A) \vee (Z = B)].$$

El axioma de extensión implica que el conjunto binario C introducido en A4 es único; se le acostumbra notar $\{A, B\}$; es decir,

$$Z \in \{A, B\} \leftrightarrow (Z = A \vee Z = B).$$

Si $A = B$, la aplicación de A4 produciría el conjunto $\{A, A\}$, el cual según A1 no es otro que $\{A\}$, o sea que también podemos formar conjuntos con un solo elemento (o unitarios).

Así, a partir de $\emptyset$ obtenemos $\{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \cdots$ y también $\{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}, \{\{\emptyset\}\}\}$, $\{\emptyset, \{\{\emptyset\}\}\}$, etc., poseyéndose muchos conjuntos, pero eso sí ninguno con más de dos elementos.

La formación de conjuntos más numerosos se logra mediante un nuevo axioma que legitime las uniones de colecciones de conjuntos.

A5 - **Axioma de la unión.**

Para toda colección $\mathfrak{C}$ de conjuntos existe otro conjunto cuyos elementos son precisamente aquellos que pertenecen al menos a uno de los conjuntos de $\mathfrak{C}$.

En el lenguaje objeto:

$$(\forall \mathfrak{C})(\exists B)(\forall Z)(Z \in B \leftrightarrow (\exists A)(A \in \mathfrak{C} \wedge Z \in A)).$$

Al igual que antes, aplicando A1 se concluye que dicho conjunto es único; lo seguiremos notando $\cup\mathfrak{C}$ o $\bigcup_{A\in\mathfrak{C}} A$ o $\bigcup\{A \mid A \in \mathfrak{C}\}$.

Usando estos dos nuevos axiomas podemos demostrar que nos es permitido formar la unión de dos conjuntos cualesquiera: Dados A, B, aplicamos A4 para obtener $\mathfrak{C} = \{A, B\}$ y luego A5 para unir los conjuntos de $\mathfrak{C}$; $\cup\mathfrak{C}$ no es otra cosa que $A \cup B$, como puede comprobarlo el lector.

Formando conjuntos unitarios o binarios y uniéndolos de dos en dos, podemos obtener conjuntos con "cualquier número" de elementos; por ejemplo, si A_1, A_2, A_3, A_4, A_5 son conjuntos distintos, nos es permitido construir $(\{A_1, A_2\} \cup \{A_3, A_4\}) \cup \{A_5\}$ para obtener el conjunto con cinco elementos $\{A_1, A_2, A_3, A_4, A_5\}$.

Si $\mathfrak{C} = \emptyset$, es decir, si no tenemos conjuntos para unir, su unión también deberá ser $\emptyset$, ya que si existiese un elemento $Z \in \cup\mathfrak{C}$, se debería cumplir $(\exists A)(A \in \emptyset \ \wedge \ Z \in A)$ lo cual es contradictorio con A2.

Para legitimar prácticamente todo lo realizado en el desarrollo intuitivo inicial del capítulo anterior, lo mismo que para llevar a cabo el trabajo del próximo capítulo, en el cual se reduce la teoría de relaciones a la teoría de conjuntos, necesitamos en este momento introducir un axioma más de la teoría de conjuntos: .

A6 - Axioma del conjunto de partes.

Para cada conjunto existe otro cuyos elementos son precisamente los subconjuntos (o partes) del conjunto dado.

En el lenguaje objeto: $(\forall X)(\exists Y)(\forall Z)(Z \in Y \leftrightarrow Z \subseteq X)$.

Una vez más el axioma de extensión garantiza la unicidad del conjunto de partes; designaremos por $\mathcal{P}(X)$ al conjunto de las partes de X. En consecuencia, $Z \in \mathcal{P}(X) \leftrightarrow Z \subseteq X$.

Queremos mencionar que todos los resultados obtenidos en el desarrollo intuitivo son demostrables con los seis axiomas dados y por este motivo en adelante los consideraremos como teoremas de nuestro estudio y los usaremos en pruebas posteriores.

Los axiomas A4, A5 y A6 han tenido como finalidad permitirnos la formación de conjuntos que no son subconjuntos de otros dados, es decir, el poder introducir conjuntos sin usar el axioma de separación; aun en estos casos usaremos la notación de llaves para designar conjuntos; por ejemplo, $\{A, B\}$ puede designarse por $\{X \mid X = A \ \vee \ X = B\}$, y $\bigcup_{A\in\mathfrak{C}} A$ puede notarse por $\{X \mid (\exists A)(A \in \mathfrak{C} \ \wedge \ X \in A)\}$ y $\mathcal{P}(X)$ por $\{Y \mid Y \subseteq X\}$.

A pesar de que poseen la forma $\{X \mid \varphi(X)\}$, debe aclararse que no se está usando indebidamente el axioma de separación, sino que la existencia del conjunto notado en la forma anterior descansa en otros axiomas; cuando haya dudas sobre la legitimidad de un determinado conjunto, las despejaremos mediante una prueba, pero en la mayoría de los casos usaremos dicha notación sin mayor justificación.

Ejercicios

1. Demuestre que $\cup\{A, B\} = A \cup B$.
   Ayuda: Use A1 y pruebe que $Z \in \cup\{A, B\} \leftrightarrow Z \in A \ \vee \ Z \in B$.

2. Diga cuáles de las siguientes proposiciones son verdaderas y cuáles no, siendo A un conjunto cualquiera:

   (a) $\emptyset \in \{\emptyset\}$.
   (b) $\emptyset \subseteq \{\emptyset\}$.
   (c) $A \in \{\{A\}, A\}$.
   (d) $\{A\} \in \{\{A\}, A\}$.
   (e) $\{A\} \subseteq \{\{A\}, A\}$.
   (f) $\emptyset \subseteq \{\{A\}, A\}$.
   (g) $\{\emptyset\} \subseteq \{\{A\}, A\}$.

+3. Demuestre por inducción que dados n conjuntos distintos, existe un conjunto cuyos elementos son precisamente los n conjuntos dados.

4. Pruebe que si $A \subseteq B$, entonces $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

5. Demuestre que $\mathcal{P}(A \cup B) \supseteq \mathcal{P}(A) \ \cup \ \mathcal{P}(B)$. ¿Qué condición puede darse para que la contenencia sea estricta?

6. Pruebe que:

   (a) $\emptyset \neq \{\emptyset\}$.
   (b) $\{\emptyset\} \neq \{\{\emptyset\}\}$.
   (c) $\{\emptyset\} \neq \{\emptyset, \{\emptyset\}\}$.

7. Demuestre que $\mathcal{P}(A \cap B) = \mathcal{P}(A) \ \cap \ \mathcal{P}(B)$ y que también en general $\mathcal{P}(\bigcap_{A\in C} A) = \bigcap_{A\in C} \mathcal{P}(A)$.

8. Pruebe que $\cup\mathcal{P}(\mathcal{C}) = \mathcal{C}$. ¿Existe alguna relación entre $\mathcal{C}$ y $\mathcal{P}(\cup\mathcal{C})$? Si su respuesta es afirmativa, pruébela.

9. Halle $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$ y $\mathcal{P}(\mathcal{P}(\mathcal{P}(\{A\})))$.

10. Demuestre que si $\mathfrak{A} \subseteq \mathfrak{B}$, entonces $\cup\mathfrak{A} \subseteq \cup\mathfrak{B}$.

**

Capítulo 3

FUNCIONES Y RELACIONES

3.1 EL PRODUCTO CARTESIANO

En el presente capítulo se estudiarán las propiedades más elementales de las funciones, de las relaciones de equivalencia y las de orden. Los tres conceptos descansan en el de "pareja ordenada", motivo por el cual lo iniciaremos con una justificación (tomada de [5]) de la definición dada por C. Kuratowski (1921), con la cual se redujo la teoría de relaciones a la teoría conjuntos, sin necesidad de introducir un nuevo axioma para caracterizar la pareja ordenada.

¿Qué es un orden? Menos ambiguamente: ¿Qué significa disponer los elementos de un conjunto en algún orden?

Supongamos que deseamos considerar los elementos (*distintos*) del conjunto $A = \{a, b, c, d\}$ en el orden $b,\ a,\ c,\ d$. Aún sin saber exactamente lo que esto significa, podemos hacer algo sensato usando conjuntos: Formemos el conjunto cuyo único elemento es el primero, luego el conjunto cuyos elementos son los dos primeros, a continuación el conjunto constituido por los tres primeros y finalmente el conjunto completo

$$\{b\}, \quad \{b, a\}, \quad \{b, a, d\}, \quad \{b, a, d, c\}\ .$$

A partir de estos cuatro conjuntos, o mejor a partir de la colección $\mathcal{O}$ formada por ellos cuatro, no importa la forma como se dispongan los conjuntos o los elementos de dichos conjuntos, podemos recuperar el orden inicialmente dado.

Por ejemplo, en

$$\mathcal{O} = \{\{a, b\},\ \{a, d, b\},\ \{b\},\ \{a, b, c, d\}\ \}$$

vemos que hay un único conjunto contenido en todos los demás y su único elemento b deberá ser el primero de la ordenación; eliminando $\{b\}$ de la colección $\mathcal{O}$, nuevamente hallamos entre los que quedan, uno incluido en los demás $\{a,b\}$, el cual contendrá los dos primeros elementos de la ordenación y como el primero fué b, necesariamente a será el segundo; eliminando de $\mathcal{O}$ los dos conjuntos anteriormente considerados $\{b\}$ y $\{a,b\}$, vemos que aún en $\{\{a,d,b\},\{a,b,c,d\}\}$ hay uno contenido en el otro, el cual deberá contener los tres primeros elementos de la ordenación y como b y a fueron los dos primeros, necesariamente d será al tercero; finalmente $\{a,b,c,d\}$ (que contiene "los cuatro primeros") determinará que c sea el cuarto de la ordenación.

En conclusión, aun cuando no sepamos lo que significa ordenar los elementos de un conjunto A, podemos asociar a cada ordenación una cierta colección $\mathcal{O}$ de subconjunto de A en forma tal que dicha colección determine sin ambigüedad la ordenación dada. Bien podríamos, al menos en cuanto a ordenaciones "totales" de conjuntos finitos se refiere, haber definido una ordenación de A como una colección tal como $\mathcal{O}$.

Apliquemos las ideas anteriores al caso de un conjunto con dos elementos $\{\triangle, \square\}$; si en la ordenación deseada aparece "$\square$" como el primer elemento, la colección $\mathcal{O}$ en cuestión sería:

$$\{\{\square\}, \{\triangle,\square\}\}$$

A este conjunto (que es una ordenación de $\{\triangle,\square\}$) lo llamaremos la "pareja ordenada" con $\square$ como primera componente y $\triangle$ como segunda componente. Formalizando un poco:

DEFINICIÓN 1. *El conjunto* $\{\{a\}, \{a,b\}\}$ *se designará en adelante por* (a,b) *y se llamará la* **pareja ordenada** *con primera componente* a *y segunda componente* b.

La definición anterior fue dada por N. Wiener y K. Kuratowski y con ella se redujo la teoría de relaciones a la teoría de conjuntos.

En vez de "componentes" se acostumbra decir "coordenadas".

A pesar de lo convincente que pueda haber sido la justificación anteriormente dada, es necesario demostrar que la pareja ordenada realmente merece su nombre:

TEOREMA 1. *La igualdad entre parejas ordenadas se tiene cuando y solamente cuando son iguales componente a componente.*

En el lenguaje objeto:

$$(\forall a)(\forall b)(\forall c)(\forall d)[(a,b) = (c,d) \leftrightarrow a = c \ \wedge \ b = d]$$ [1]

Demostración.

(i) Si $a = c \wedge b = d$, entonces por A1 se tiene $\{a\} = \{c\} \wedge \{a,b\} = \{c,d\}$, luego $\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$ o sea $(a,b) = (c,d)$.

(ii) Recíprocamente si $(a,b) = (c,d)$,

a) Supongamos que $a = b$. Entonces $\{a,b\} = \{a,a\} = \{a\}$, de donde

$$(a,b) = \{\{a\},\{a,b\}\} = \{\{a\},\{a\}\} = \{\{a\}\}.$$

Como $(a,b) = (c,d)$, se tendrá $\{\{a\}\} = \{\{c\},\{c,d\}\}$ y por A1 se cumplirá que $\{c\} = \{a\} \ \wedge \ \{c,d\} = \{a\}$, de donde $c = a = d$.

Intercambiando los papeles de (a,b) y (c,d) se obtiene la misma conclusión, es decir que si una de las parejas ordenadas posee sus dos componentes iguales, la otra también las poseerá y $a = b = c = d$; en particular $a = c \ \wedge \ b = d$.

b) Supongamos $a \neq b$; de lo anterior se sigue que también $c \neq d$; como $(a.b) = (c,d)$ o sea $\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$, siendo $\{a\}$ un conjunto unitario, por A1 deberá existir también en el conjunto de la derecha un conjunto unitario y éste no puede ser $\{c,d\}$ ya que $c \neq d$, luego $\{a\} = \{c\}$ y por A1, $a = c$. Análogamente se debe concluir que $\{a,b\} = \{c,d\}$ y como $a = c$ y $a \neq b$ y $c \neq d$, entonces $b = d$.

□

COROLARIO 1. $(\forall a,b)(a \neq b \rightarrow (a,b) \neq (b,a))$.

Es evidente después del teorema anterior ya que (a,b) y (b,a) no tienen en este caso iguales entre sí sus primeras componentes (ni sus segundas).

Para el lector es conocido el plano provisto de un sistema de coordenadas cartesianas; como en él un punto está determinado por (y determina a su vez) sus coordenadas, dicho plano puede identificarse con el conjunto de todas las parejas ordenadas cuyas componentes son números reales. Generalizando un poco podemos preguntarnos: Dados dos conjuntos A, B, ¿existe un conjunto constituido por todas las parejas ordenadas que puedan formarse de manera que su primera componente sea elemento de A y su

[1] En adelante en vez de $(\forall a)(\forall b)(\forall c)(\forall d)(\varphi...)$ escribiremos $(\forall a,b,c,d)\ (\varphi...)$.

segunda de B? La respuesta es afirmativa y lo que sigue está dedicado a su demostración.

Si $Z = (X,Y)$ con $X \in A$ y $Y \in B$, es decir, si
$(\exists X)(\exists Y)(X \in A \ \wedge \ Y \in B \ \wedge \ Z = (X,Y))$, se tiene que
$\{X\} \subseteq A \subseteq A \cup B$ y $\{X,Y\} \subseteq A \cup B$ y por A6,
$\{X\} \in \mathcal{P}(A \cup B)$ y $\{X,Y\} \in \mathcal{P}(A \cup B)$, luego $\{\{X\},\{X,Y\}\} \subseteq \mathcal{P}(A \cup B)$
y nuevamente por A6, $\{\{X\},\{X,Y\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$ o sea que

$$(\alpha) \qquad Z = (X,Y) \in \mathcal{P}(\mathcal{P}(A \cup B)) \quad \text{si} \quad X \in A \quad \text{y} \quad Y \in B.$$

Sabemos ahora que existe un conjunto, $\mathcal{P}(\mathcal{P}(A \cup B))$, que contiene entre sus elementos a todas las parejas ordenadas con primera coordenada en A y segunda en B. Luego, usando los axiomas de separación y de extensión podemos a partir de $\mathcal{P}(\mathcal{P}(A \cup B))$, formar el único conjunto (notado $A \times B$) constituido por todas las parejas ordenadas con primera componente en A y segunda en B. Resumiendo:

TEOREMA 2. *Para A, B conjuntos cualesquiera, existe un único conjunto constituido por todas las parejas ordenadas que pueden formarse tomando su primera coordenada de A y su segunda de B.*

DEFINICIÓN 2. *El conjunto cuya existencia se afirma en el teorema anterior, se llama el producto cartesiano de A por B y se nota $A \times B$.*

Para lectores suspicaces entraremos un poco más en los detalles técnicos:

$A \times B$ se obtiene separando de $\mathcal{P}(\mathcal{P}(A \cup B))$ aquellos elementos Z que cumplen la condición "Z es una pareja ordenada con primera componente en A y segunda en B", la cual redactada correctamente en lenguaje objeto, toma la forma

$$(\exists X)(\exists Y)(X \in A \ \wedge \ Y \in B \ \wedge \ Z = (X,Y)$$

Es decir, $Z \in A \times B$ si y sólo si
$Z \in \mathcal{P}(\mathcal{P}(A \cup B)) \ \wedge \ (\exists X,Y)(X \in A \ \wedge \ Y \in B \ \wedge Z = (X,Y))$ o lo que es lo mismo:

$$(\beta) \qquad A \times B = \{Z \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid (\exists X)(\exists Y)(X \in A \ \wedge \ Y \in B \ \wedge Z = (X,Y))\}$$

Pero de $\varphi(Z) = (\exists X)(\exists Y)(X \in A \ \wedge \ Y \in B \ \wedge Z = (X,Y))$ se dedujo $Z = (X,Y) \in \mathcal{P}(\mathcal{P}(A \cup B))$ (ver (α)) o sea que
$\varphi(Z) \rightarrow Z \in \mathcal{P}(\mathcal{P}(A \cup B)) \wedge \varphi(Z)$; siendo evidente la implicación recíproca, se obtiene que

$$Z \in A \times B \leftrightarrow (\exists X)(\exists Y)(X \in A \ \wedge \ Y \in B \ \wedge \ Z = (X,Y)).$$

Siguiendo lo dicho en el útimo párrafo del capítulo anterior, en vez de (β) escribiremos en adelante:

$$A \times B = \{Z \mid (\exists X)(\exists Y)(X \in A \ \wedge \ Y \in B \ \wedge \ Z = (X,Y))\}$$

o más brevemente (siguiendo la costumbre):

$$A \times B = \{(X,Y) | X \in A \ \wedge \ Y \in B\},$$

o lo que es lo mismo:

$$(X,Y) \in A \times B \leftrightarrow X \in A \ \wedge \ Y \in B.$$

TEOREMA 3. *Si A, B, C, D son conjuntos cualesquiera, se cumple que*

(a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

(b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

(c) $A \times (B - C) = (A \times B) - (A \times C)$.

Demostración. A modo de ejemplo, probaremos solamente (c) y dejaremos al lector como ejercicio, la demostración de las otras dos propiedades:

$$\begin{aligned}
(X,Y) \in (A \times B - A \times C) &\leftrightarrow \\
&\leftrightarrow (X,Y) \in A \times B \wedge (X,Y) \notin A \times C \\
&\leftrightarrow (X \in A \wedge Y \in B) \wedge \neg(X \in A \wedge Y \in C) \\
&\leftrightarrow (X \in A \wedge Y \in B) \wedge (X \notin A \vee Y \notin C) \\
&\leftrightarrow \underbrace{((X \in A \wedge Y \in B) \wedge X \notin A)}_{p} \\
&\quad \vee ((X \in A \wedge Y \in B) \wedge Y \notin C) \\
&\leftrightarrow (X \in A \wedge Y \in B) \wedge Y \notin C \text{ (ya que } p \text{ es falsa)} \\
&\leftrightarrow X \in A \wedge (Y \in B \wedge Y \notin C) \\
&\leftrightarrow X \in A \wedge Y \in B - C \\
&\leftrightarrow (X,Y) \in A \times (B - C).
\end{aligned}$$

□

Cuando uno cualquiera de los conjuntos A, B es vacío, nuestra intuición nos dice que no podemos formar parejas ordenadas con primera componente en A y segunda en B.

TEOREMA 4. $A \times B = \emptyset \leftrightarrow (A = \emptyset \ \vee \ B = \emptyset)$

En vez de demostrarlo directamente, probaremos la equivalencia entre sus negaciones:

$$(A \times B) \neq \emptyset \leftrightarrow (A \neq \emptyset \ \wedge \ B \neq \emptyset)$$

En efecto:

$$\begin{aligned} A \neq \emptyset \ \wedge \ B \neq \emptyset &\leftrightarrow (\exists X)(X \in A) \ \wedge \ (\exists Y)(Y \in B) \\ &\leftrightarrow (\exists X)(\exists Y)(X \in A \ \wedge \ Y \in B) \\ &\leftrightarrow (\exists X)(\exists Y)((X,Y) \in A \times B) \\ &\leftrightarrow (A \times B) \neq \emptyset \, . \end{aligned}$$

De la definición dada de producto cartesiano se deduce que todo subconjunto de un producto cartesiano es un conjunto de parejas ordenas; podemos preguntarnos si es cierta la proposición recíproca: ¿Es todo conjunto de parejas ordenas subconjunto de algún producto cartesiano?

Nuestra intuición nuevamente nos dice que la respuesta es afirmativa. Por ejemplo, si $R = \{(a,b),(1,a),(\triangle,3),(a,3)\}$, podemos tomar como A el conjunto constituido por las primeras componentes de las parejas de R y como B el de las segundas componentes; así:

$$A = \{a, 1, \triangle\}, \qquad B = \{b, a, 3\} \qquad \text{y} \qquad R \subseteq A \times B$$

Aquí A y B son los conjuntos "más pequeños" adecuados para nuestro propósito, pero también hubiesen servido otros conjuntos "mayores" ya que si $A \subseteq M$ y $B \subseteq N$ entonces $R \subseteq M \times N$ (pues $A \times B \subseteq M \times N$); ¿se puede tomar $M = A \cup B = N$?

Pero nos encontramos en un verdadero problema: de acuerdo con los axiomas dados y los resultados obtenidos, ¿cómo formamos "legítimamente" A y B?

A es el conjunto de los elementos que cumplen la condición "X es primera componente de una pareja de R", o sea "existe una pareja en R con X como primera componente", lo cual se puede traducir en el lenguaje objeto por $(\exists Y)((X,Y) \in R)$. Análogamente B está caracterizado por $(\exists X)((X,Y) \in R)$. Pero, ¿de qué conjunto (o conjuntos) podemos separar los elementos que cumplen estas condiciones? Si recordamos que (a,b) es la colección $\{\{a\},\{a,b\}\}$ y se nos ocurre formar la unión de esta colección, tenemos casi resuelto el problema, ya que

$$\cup(a,b) = \{a\} \cup \{a,b\} = \{a,b\}$$

es un conjunto que posee como elementos tanto a la primera como a la segunda componente de (a,b). Para obtener el conjunto buscado bastará entonces unir previamente todas las parejas de R.

En el ejemplo,

$$\begin{aligned} \cup R = &\bigcup_{(X,Y)\in R} (X,Y) = \{\{a\},\{a,b\}\} \cup \{\{1\},\{1,a\}\} \\ &\cup \{\{\triangle\},\{\triangle,3\}\} \cup \{\{a\},\{a,3\}\} \\ =&\{\{a\},\{a,b\},\{1\},\{1,a\},\{\triangle\},\{\triangle,3\},\{a\},\{a,3\}\}. \end{aligned}$$

Uniendo esta última colección obtenemos

$$\cup(\cup R) = \bigcup\left(\left(\bigcup_{(X,Y)\in R}(X,Y)\right)\right) = \{a,b,1,\triangle,3\}$$

el cual es el conjunto formado precisamente por todos los elementos que figuran como primeras o como segundas componentes de las parejas ordenadas de R.

Resumiendo e introduciendo alguna terminología:

DEFINICIÓN 3. *Una relación (binaria) es un conjunto de parejas ordenadas.*

TEOREMA 5. *Toda relación es un subconjunto de un producto cartesiano.*

Demostración. Sea R una relación; después de la definición anterior y del análisis que precedió, $R \subseteq (\cup(\cup R)) \times (\cup(\cup R))$ quedando demostrado. □

DEFINICIÓN 4. *El conjunto $\cup(\cup R)$ se llama el campo de la relación R y se nota $\tau(R)$.*

Así $\tau(R)$ viene a estar constituido por todos los elementos que son primeras o segundas componentes de las parejas de R.

DEFINICIÓN 5. *Se llama* dominio *de un relación R al conjunto de las primeras componentes de las parejas de R; se nota $\mathcal{D}(R)$.*

Según lo dicho, $\mathcal{D}(R) = \{X \in \tau(R) : (\exists Y)((X,Y) \in R)\}$.

DEFINICIÓN 6. *Se llama recorrido de una relación al conjunto de las segundas componentes de las parejas de la relación; se nota $\mathcal{D}(R)$.*

Entonces $\mathcal{R}(R) = \{Y \in \tau(R) | (\exists X)((X,Y) \in R)\}$

Además según lo dicho, $R \subseteq \mathcal{D}(R) \times \mathcal{R}(R)$

Hemos desarrollo en esta sección el material necesario para (como lo dijimos al comienzo) reducir la teoría de relaciones a la de conjuntos. Creemos que se ha dado una motivación suficiente para que el lector encuentre más o menos "natural" la definición dada de pareja ordenada, pero, ni todos los matemáticos ni todos los lectores gustan de ella, debido a que intuitivamente es molesto y fastidioso el que se tengan propiedades como $\{a,b\} \in$(a,b)y $(a,b) \in \mathcal{P}(\mathcal{P}(\{a,b\}))$; sin embargo, si el lector lo desea, puede olvidar hechos como los anteriores, que son realmente secundarios y retener solamente los resultados fundamentales para todo el desarrollo posterior:

(i) $(a,b) = (c,d) \leftrightarrow [a = c \wedge b = d]$.

(ii) Podemos formar el producto cartesiano de dos conjuntos cualesquiera.

(iii) Los elementos de un conjunto son parejas ordenadas si y solamente si el conjunto es un subconjunto de un producto cartesiano.

(iv) Dada una relación, siempre se puede formar su campo, su dominio y su recorrido.

Ejercicios

1. Pruebe que $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$ y que si $A \subseteq M$ y $B \subseteq N$, entonces $A \times B \subseteq M \times N$.

2. Demuestre que si $\mathfrak{A}$ y $\mathfrak{B}$ son colecciones de conjuntos,

   (a)
   $$M \times \left(\bigcup_{A \in \mathfrak{A}} A \right) = \bigcup_{A \in \mathfrak{A}} (M \times A)$$

   (b)
   $$\left(\bigcup_{A \in \mathfrak{A}} A \right) \times \left(\bigcup_{B \in \mathfrak{B}} B \right) = \bigcup_{A \in \mathfrak{A}} \left(\bigcup_{B \in \mathfrak{B}} (A \times B) \right) = \bigcup_{(A,B) \in \mathfrak{A} \times \mathfrak{B}} A \times B$$

3. (a) Una manera de introducir la definición de relación es
   $$R \text{ es una relación} \Leftrightarrow \varphi$$
   donde φ es una f.b.f. del lenguaje objeto; halle φ.

   (b) Enuncie en el lenguaje objeto el teorema "Toda relación es un subconjunto de un producto cartesiano"

4. Siguiendo las ideas expuestas en esta sección, dé una definición adecuada de "tripla" ordenada, demostrando que cuando las triplas están formadas por elementos distintos,
   $$(a,b,c) = (p,q,r) \leftrightarrow a = p \wedge b = q \wedge c = r.$$

5. Si en vez de lo sugerido para el ejercicio 4, se hubiese tomado como "tripla" $((a,b),c)$ o $(a,(b,c))$, pruebe que también en estos casos se cumple la equivalencia pedida.

*6. En adelante consideraremos $(a_1, a_2, a_3, ..., a_n)$ como
   $$(...((a_1, a_2), a_3)..., a_n).$$
   Pruebe que en este caso, para cualquier $n \geq 3$,
   $$(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n) \leftrightarrow a_1 = b_1 \wedge a_2 = b_2 \wedge \cdots \wedge a_n = b_n.$$
   En concordancia con lo dicho, en adelante siempre el producto cartesiano $A_1 \times A_2 \times A_3 \times ... \times A_n$ se entenderá como
   $$(...(((A_1 \times A_2) \times A_3) \times A_4)... \times A_n).$$

3.2 RELACIONES

En la sección anterior por los motivos expuestos al final, nos hemos apresurado a definir "relación" como un conjunto de parejas ordenadas; dicha definición posiblemente no esté de acuerdo con nuestro concepto intuitivo de relación. En la vida diaria se entiende por relación algo como el vínculo que existe entre padres e hijos, entre esposos, etc. Sin embargo queremos hacer notar la correspondencia que existe entre nuestra definición y las relaciones presentadas bajo formas como

(a) X escribió la obra Y,

(b) X es hijo de Y,

(c) X es hombre, Y es mujer y X es esposo de Y,

(d) X mide Y cm. de estatura,

las cuales relacionan respectivamente el autor con su obra, los hijos con sus padres, el esposo con su esposa y a una persona con su estatura.

Lo primero que debemos hacer es precisarlas, especificando para cada una de ellas los conjuntos donde toman valores X y Y, sus referenciales, digamos. En (a) el referencial para X debe ser un conjunto A de personas y el para Y un conjunto B de títulos de obras literarias; en (b) y (c) los referenciales A y B deben ser conjuntos de personas y en (d) el referencial A para X debe ser un conjunto de personas y el B para Y un conjunto de números reales positivos.

Concretemos los referenciales A y B para el ejemplo (a):
$A = \{$Cervantes, Shakespeare, P. Neruda, G. García Márquez$\}$ y
$B = \{$Otelo, La Gitanilla, Hamlet, Cien años de Soledad, Doña Bárbara, El Quijote, El rey Lear$\}$

La relación "X escribió la obra Y" entre los elementos de los conjuntos A y B anteriores, nos permite formar parejas ordenadas tomando como primera componente uno de los autores y como segunda una de las obras de B que haya sido escrita por él. En otra palabras, podemos separar de $A \times B$ aquellas parejas ordenadas cuya primera componente está en la relación dada con la segunda, es decir, formemos el conjunto

$$R = \{(X, Y) \in A \times B \mid X \text{ escribió } Y\}.$$

En el ejemplo éste sería

$R = \{$(Cervantes, La Gitanilla), (Cervantes, El Quijote), (Shakespeare, Otelo), (Shakespeare, Hamlet), (Shakespeare, El rey Lear), (G. García M., Cien años de Soledad)$\}$.

De esta manera, a toda "relación" dada en la forma usual entre lo elementos de dos conjuntos, se le hace corresponder un único conjunto de parejas ordenadas; por este motivo podemos considerar que la relación es en realidad el conjunto de parejas ordenadas; además en casos como el del ejemplo anterior, a partir del conjunto R se puede intuir la relación entre autor y obra.

DEFINICIÓN 7. *Si $R \subseteq A \times B$, se acostumbra decir que R es una relación de A en B; A se llama la* **fuente** *y B la* **meta** *de R. Si $R \subseteq A \times A$ se dice que R es una relación en A. Si $(X, Y) \in R$, diremos que X* **está relacionado con** *Y mediante R y escribiremos XRY.*

Por ejemplo, como $\emptyset$ es subconjunto de todo conjunto, $\emptyset$ es una relación de A en B, cualesquiera sean A y B.

Si X es un conjunto, entonces $\{(Z, W) \in X \times X \mid Z = W\}$ es la relación de igualdad en X.

A partir de una relación R siempre es posible construir otra llamada su *relación inversa*; simplemente se invierten las componentes de las parejas de R. Formalmente: Dada una relación R, formemos $\mathcal{D}(R)$ y $\mathcal{R}(R)$ y luego $\mathcal{R}(R) \times \mathcal{D}(R)$; separemos de este último conjunto las parejas (Y, X) tales que $(X, Y) \in R$, es decir,

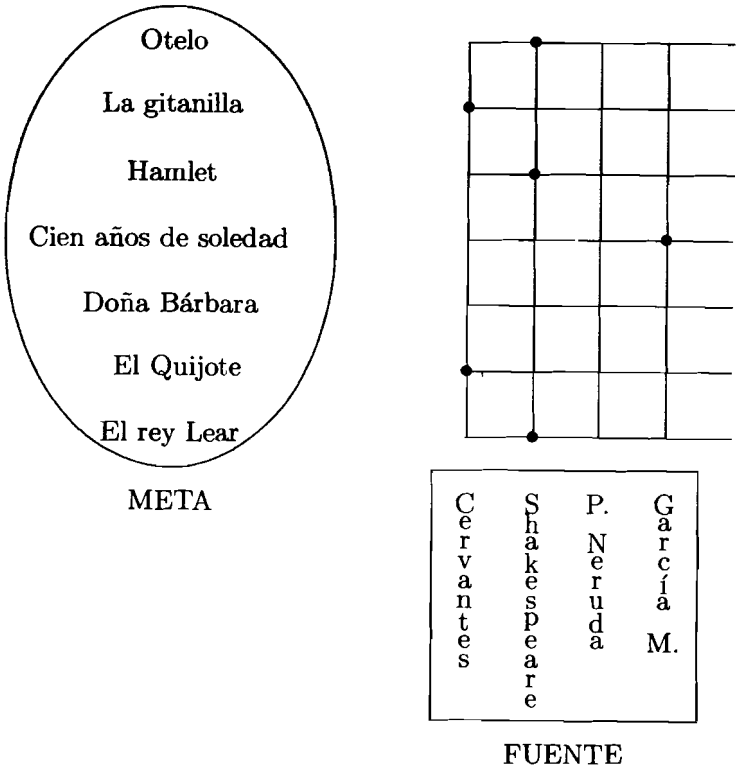
$$R^{-1} = \{(Y, X) \in \mathcal{R}(R) \times \mathcal{D}(R) | (X, Y) \in R\}$$

Entonces $(Y, X) \in R^{-1} \leftrightarrow (Y, X) \in \mathcal{R}(R) \times \mathcal{D}(R) \wedge (X, Y) \in R$; pero es fácil demostrar que $(X, Y) \in R \rightarrow (Y, X) \in \mathcal{R}(R) \times \mathcal{D}(R)$ de manera que $(Y, X) \in R^{-1} \leftrightarrow (X, Y) \in R$ y así

$$R^{-1} = \{(Y, X) | (X, Y) \in R\}.$$

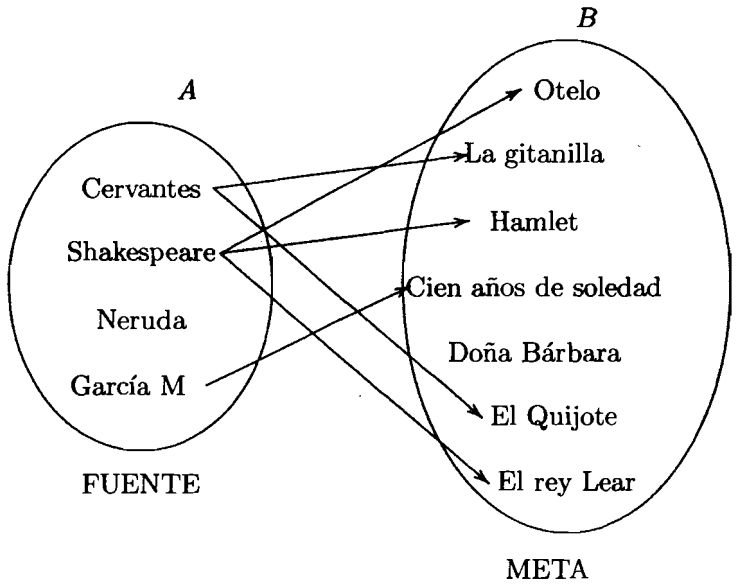
Muchas veces es de utilidad visualizar las relaciones mediante gráficas o diagramas. Para representarlas gráficamente se imita lo que generalmente se hace con un sistema de coordenadas cartesianas en el plano: Si R es una relación de A en B, se acostumbra trazar una vertical por cada elemento de A y una horizontal por cada elemento de B; sobre los cruces se marcan los puntos correspondientes a las parejas de la relación, teniéndose presente la prioridad (en el orden) que se dá a los elementos de la fuente sobre los

de la meta. Así la relación "X escribió la obra Y" del ejemplo (a) anterior se puede representar gráficamente como se muestra a continuación:



Mediante un diagrama se puede dar una "representación sagital" de una relación en la forma siguiente: Coloquemos dentro de una curva cerrada los elementos del conjunto fuente y dentro de otra (generalmente a la derecha de la anterior) los del conjunto meta. Si un elemento X de A está relacionado con otro Y de B, tracemos una flecha de X hacia Y. El diagrama que aparece a continuación corresponde a la representación sagital de la misma

relación "X escribió la obra Y".



Ejercicios

1. Tome como A un conjunto específico de útiles de escritorio de no más de diez elementos y como B el de los números reales; considérese la relación "X vale Y pesos" de A en B. Averiguando los precios vigentes, forme el conjunto de parejas ordenadas determinado por esta relación. Represéntela sagital y gráficamente.

2. Considere la relación "$X \in Y$" de $\{A, B, C\}$ en $\mathcal{P}(\{A, B, C\})$. Forme el conjunto de parejas ordenadas determinando por esta relación y represéntela sagitalmente.

*3. Represente gráficamente las relaciones siguientes:

   (a) $R_1 = \{(X, Y) \in [-2, 3] \times [0, 7] : X^2 = Y\}$.
   (b) $R_2 = \{(x, y) \in [0, 2\pi] \times \mathbb{R} : \text{sen(x)} = y\}$.
   (c) $R_3 = \{(X, Y) \in \mathbb{R} \times \mathbb{R} : |X| + |Y| \leq 1\}$.

4. Para cada una de las relaciones siguientes, halle explícitamente el conjunto de parejas ordenadas y represéntelo sagitalmente:

(a) "X es hijo de Y", considerada en el conjunto formado por usted, sus hermanos, padres, abuelos y bisabuelos.

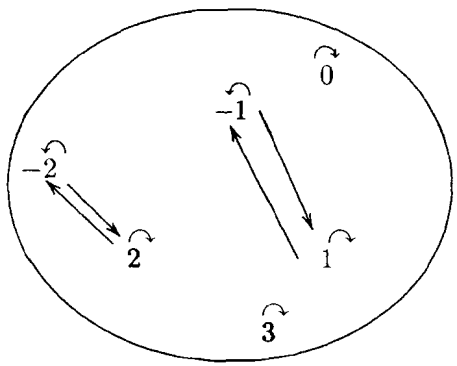
(b) $\{(X,Y) \in A \times A \mid X \leq Y\}$ donde $A = \{1,2,3,6,7\}$.

(c) $\{(X,Y) \in A \times A \mid X$ es divisor de $Y\}$ definida en el conjunto $A = \{1,2,3,4,5,6,10,12\}$.

5. Represente sagitalmente la relación

$$\{(X,Y) \in \mathcal{P}(\{a,b,c\}) \times \mathcal{P}(\{a,b,c\}) \mid X \subseteq Y\}.$$

6. Cuando se tiene una relación definida en un conjunto A, como "X posee el mismo valor absoluto que Y" en $A = \{-2,-1,0,1,2,3\}$, en vez de efectuar una representación sagital tomando dos copias de A y trazando flechas de la copia fuente hacia la copia meta, se acostumbra representar una sola vez al conjunto A y entre sus elementos relacionados se trazan flechas que van de la primera componente de la pareja a la segunda. Véase en la gráfica siguiente la representación de "$|X| = |Y|$".



¿Qué significan los bucles ($\curvearrowright$)?

Represente en esta misma forma las relaciones de los ejercicios anteriores 2., 4. y 5.

7.

(a) Como la relación inversa R^{-1} se forma simplemente intercambiando entre sí primeras y segundas componentes de las parejas de R o lo que es lo mismo, intercambiando X con Y cuando R se define mediante una expresión de la forma $\varphi(X,Y)$, aplique esta técnica (con las precauciones del caso) para formar la relación inversa de cada una las relaciones de los ejercicios 3., 4. y 5.

(b) Represente gráficamente las relaciones inversas de las dadas en el ejercicio 3. y sagitalmente (en la forma descrita en el ejercicio 6.) las inversas de las relaciones consideradas en los ejercicios 4. y 5.

(c) Comparando las representaciones sagitales de R^{-1} anteriormente pedidas con las de R, deduzca un método para hallar directamente la representación sagital de R^{-1} a partir de la de R.

8. A manera de discusión informal: nuestra definición oficial de relación ha sido "conjunto de parejas ordenadas" o "subconjunto de un producto cartesiano". Pero hemos visto que muchas relaciones pueden obtenerse separando de un producto cartesiano aquellas parejas ordenadas que satisfacen una condición en dos variables $\varphi(X,Y)$, como "$X \neq Y$", "X es hijo de Y", etc. Nos preguntamos ¿será cierto que toda relación puede obtenerse de esta manera? Particularizando: dada $R \subseteq \mathbb{N} \times \mathbb{N}$, existirá una condición en dos variables $\varphi(X,Y)$ tal que

$$R = \{(X,Y) \in \mathbb{N} \times \mathbb{N} | \varphi(X,Y)\}?$$

9. Si R es cualquier relación, ¿es siempre $(R^{-1})^{-1}$ igual a R?

3.3 FUNCIONES

Debido a que ya es práctica común definir una función como una cierta relación, lo haremos de esta manera, sin previas justificaciones.

DEFINICIÓN 8. *Una función es una relación en la cual no existen dos o más parejas distintas con la misma primera componente; o lo que es lo mismo: f es una función $\Leftrightarrow$ f es una relación y*

$$(\forall x, y, z)((x, y) \in f \wedge (x, z) \in f \rightarrow y = z).$$

Por ejemplo, $f = \{(1,2),(2,2),(3,1),(4,3)\}$ es una función.

Su dominio es $\mathcal{D}(f) = \{1,2,3,4\}$ y su recorrido es $\mathcal{R}(f) = \{1,2,3\}$.

La relación $R = \{(2,1),(2,2),(a,b)\}$ no es una función ya que las parejas ordenadas (2,1) y (2,2) poseen la misma primera componente.

DEFINICIÓN 9. *Una función de A en B es una función f tal que*

i) $\mathcal{D}(f) = A$ *y*

ii) $\mathcal{R}(f) \subseteq B$.

En otras palabras, una función de A en B es una relación f de A en B tal que *todo* elemento de A está relacionado (por f) con *un único* elemento de B.

Debido a este hecho, es costumbre notar por $f(x)$ a este único elemento de B con el cual x está relacionado mediante f y escribir $y = f(x)$ en vez de $(x,y) \in f$. Se dice que y (o que $f(x)$) es la imagen por f de x, o el valor tomado por f en x.

Una función es simplemente un conjunto de parejas ordenadas tal que en éstas todas sus primeras componentes son distintas. En cambio, una función de A en B (o una aplicación de A en B), es una tripla ordenada (f, A, B) en la cual $A = \mathcal{D}(f)$ y $B \supseteq \mathcal{R}(f)$. Por este motivo es costumbre notarla $f : A \rightarrow B$, $A \xrightarrow{f} B$,ó $f : A \mapsto B$, con $x \rightarrow f(x)$, o algo semejante. Al conjunto B se le llama comúnmente la *meta de f, el conjunto de llegada de f o el codominio de f.*

Ejemplos de funciones.

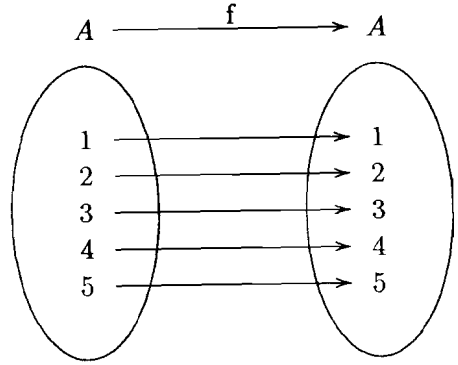
1. Si $A = \{0,1,2,3\}$ y $B = \{0,1,2,3,4,5,6,7,8,9,10\}$ entonces el conjunto de parejas $f = \{(0,0), (1,1), (2,4), (3,9)\}$ es una función de A en B. También se hubiese podido definir en la forma

$$f : A \rightarrow B \quad \text{ó} \quad f : A \rightarrow B \quad \text{tal que} \quad y = f(x) = x^2$$
$$x \rightarrow x^2$$
$$\text{ó} \qquad f = \{(x, x^2) \mid x \in A\} \qquad \text{de } A \text{ en } B.$$

2. Si $A = B = \{1,2,3,4,5\}$, entonces

$$f = \{(1,1),(2,2),(3,3),(4,4),(5,5)\}$$

es una función de A en A. Representémosla mediante su diagrama sagital: (ver la siguiente gráfica)



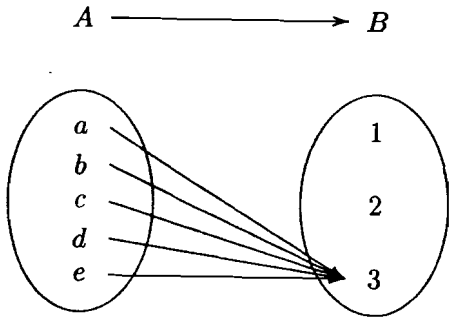
Observamos que a cada elemento de A se le hace corresponder precisamente él mismo. Por esto se le acostumbra llamar la *función idéntica* de A o la *identidad de A* y se le representa por I_A. Generalizando: Si A es un conjunto cualquiera, se llama la identidad de A a la función $I_A : A \rightarrow A$ tal que para todo elemento x de A, se tiene que $I_A(x) = x$.

3. Si A es subconjunto de B, a la función

$$j : A \rightarrow B$$
$$x \rightarrow x$$

se le acostumbra llamar la *inyección canónica de A en B*, debido a que su oficio es inyectar A dentro de B.

4. Sean $A = \{a, b, c, d, e\}$ y $B = \{1, 2, 3\}$. A la función de A en B que posee como diagrama sagital



se le llama una función constante, debido a que toma el mismo valor en todos los elementos de A.

Generalizando: Una función $f : A \to B$ con $B \neq \emptyset$ se llama una *función constante*, si existe $b_0 \in B$ tal que $f(x) = b_0$, cualquiera sea x en A.

Nótese que aun cuando todos los elementos de A tienen la misma imagen, no se está violando la definición de función ya que cada elemento de A sigue estando relacionado con un único elemento de B. Lo que la definición prohibe es que algún elemento de A esté relacionado con dos o más de B.

5. Al igual que con las relaciones, también se pueden utilizar condiciones adecuadas en dos variables para definir funciones.
Por ejemplo si

$A = \{\text{Bogotá, Roma, París, Caracas, Cali}\}$ y

$B = \{\text{Italia, Venezuela, Colombia, Inglaterra, Francia}\}$,

entonces "x está situado en el país y" es una función de A en B.

6. Suponemos que el lector está familiarizado con los números reales. Vamos a considerar algunas funciones entre subconjuntos de $\mathbb{R}$.

   a) La aplicación $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$.

   b) La función $g : [0, +\infty) \to [0, +\infty)$ definida por $g(x) = x^2$.

Nótese que $f \neq g$ puesto que poseen dominios y codominios diferentes. Además si pensamos en nuestra definición inicial de función, $g \subset f$.

   c) Las primeras funciones trigonométricas

$$\begin{array}{lll} \mathbb{R} \to \mathbb{R} & \mathbb{R} \to \mathbb{R} & (-\pi/2, \pi/2) \to \mathbb{R} \\ x \mapsto sen\ x, & x \mapsto cos\ x, & x \mapsto tg\ x \end{array}$$

Como ejercicio, el lector debe representarlas gráficamente en un sistema de coordenadas cartesianas.

7. Sean A, B conjuntos cualesquiera; las funciones

$$\begin{array}{ll} P_{r_1} : A \times B \to A & P_{r_2} : A \times B \to B \\ (x, y) \mapsto x & (x, y) \mapsto y \end{array}$$

se llaman primera y segunda proyección, respectivamente, o proyección sobre la primera coordenada y proyección sobre la segunda coordenada.

8. Si $f : A \to B$ y $g : C \to D$, a partir de ellas se puede construir otra función notada $f \times g$ de $A \times B$ en $B \times D$ de la siguiente manera:

$$(f \times g)(x, y) = (f(x), g(y)).$$

Si su conciencia se lo exige, demuestre que realmente es una función.

Si $f : A \to B$ y $g : C \to D$, se puede pensar que $f \cup g$ (unión de conjuntos de parejas ordenadas) es una función de $A \cup C$ en $B \cup D$. pero esto no siempre es así: Como se prueba fácilmente, $\mathcal{D}(f \cup g) = \mathcal{D}(f) \cup \mathcal{D}(g) = A \cup C$ y $\mathcal{R}(f \cup g) = \mathcal{R}(f) \cup \mathcal{R}(g) \subseteq B \cup D$, de modo que la única falla radica en que algunas veces $f \cup g$ no es función, puesto que se puede tener $(x, y) \in f$ y $(x, z) \in g$ con $z \neq y$ y entonces $(x, y) \in f \cup g$ y $(x, z) \in f \cup g$.

Para que $f \cup g$ sea función es necesario que f y g coincidan en los elementos comunes de sus dominios: Si $x \in \mathcal{D}(f) \cap \mathcal{D}(g)$ entonces $f(x) = g(x)$. Esta condición en particular se cumple si los dominios son disyuntos.

TEOREMA 6. *Sean $f : A \to B$ y $g : C \to D$; si $A \cap C = \emptyset$, entonces $f \cup g$ es una función de $A \cup C$ en $B \cup D$.*

Demostración. Una demostración más rutinaria sería:

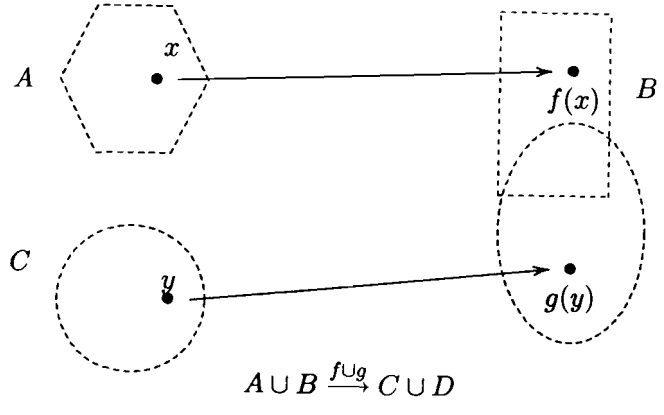
$$\begin{aligned}&(x,y) \in f \cup g \ \wedge \ (x,z) \in f \cup g\\ &\leftrightarrow [(x,y) \in f \ \vee \ (x,y) \in g] \wedge [(x,z) \in f \vee (x,z) \in g]\\ &\leftrightarrow [(x,y) \in f \wedge (x,z) \in f] \vee [(x,y) \in f \wedge (x,z) \subset g]\\ &\vee [(x,y) \in g \wedge (x,z) \in f] \vee [(x,y) \in g \wedge (x,z) \in g]\end{aligned}$$

Siendo disyuntos los dominios de f y g, las posibilidades 2a. y 3a. son falsas, así que se deduce

$$[(x,y) \in f \wedge (x,z) \in f] \vee [(x,y) \in g \wedge (x,z) \ \in g]$$

Como f y g son funciones, en ambos casos se concluye $y = z$, quedando demostrado que $f \cup g$ es función.

Observemos cómo se calcula $f \cup g$ en este caso: Si $x \in A \cup B$, entonces $x \in A \veebar x \in B$ (es "o exclusivo" debido a que $A \cap B = \emptyset$). Si $x \in A$, la pareja ordenada con x como primera componente de $f \cup g$ es la que está en f, es decir, $(f \cup g)(x) = f(x)$. Análogamente, si $x \in B$, entonces $(f \cup g)(x) = g(x)$.



Nótese que si además $A \cap C = \emptyset$, entonces $f \cap g = \emptyset$. □

DEFINICIÓN 10. *Diremos que una función f de A en B es* uno a uno *o inyectiva (o que es una* inyección*) si elementos distintos de A tienen imágenes distintas mediante f; es decir*

$$f \text{ es inyectiva } \rightarrow (\forall u, v \in \mathcal{D}(f)) \quad (u \neq v \rightarrow f(u) \neq f(v)).$$

Algunas veces es útil usar la forma contrarrecíproca de la última implicación: $f(u) = f(v) \rightarrow u = v$.

Las funciones de los ejemplos 1) y 2) son inyectivas, como puede verse por simple inspección; también lo es la del ejemplo 3) puesto que si $u \neq v, j(u) = u \neq v = j(v)$; la función correspondiente al diagrama sagital del ejemplo 4) no es uno a uno debido a que todos los elementos poseen como imagen el número 3; la aplicación $f : \mathbb{R} \rightarrow \mathbb{R}$ dada por $f(x) = x^2$ no es una inyección ya que en particular $f(-2) = (-2)^2 = 4 = 2^2 = f(2)$ y $-2 \neq 2$; en cambio $g : [0, +\infty) \rightarrow [0, +\infty)$ definida por $g(x) = x^2$, sí es inyectiva puesto que si $g(u) = u^2 = v^2 = g(v)$, entonces $|u| = |v|$ y como $u, v \geq 0$, se tiene que $|u| = u$ y $|v| = v$, luego $u = v$ (hemos empleado la forma contrarrecíproca de la definición).

TEOREMA 7. *Si $f : A \rightarrow B$ y $g : C \rightarrow D$ son funciones inyectivas, entonces también lo es*

$$\begin{aligned}f \times g : A \times C &\rightarrow B \times D\\ (x,y) &\mapsto (f(x), g(y)).\end{aligned}$$

Demostración. Supongamos $(f \times g)(x,y) = (f \times g)(u,v)$ o sea $(f(x), g(y)) = (f(u), g(v))$ de donde $f(x) = f(u) \wedge g(y) = g(v)$ y como f y g son inyectivas, $x = u \wedge y = v$, luego $(x,y) = (u,v)$. □

Con respecto a $f \cup g$ tenemos el resultado siguiente:

TEOREMA 8. *Si $f : A \rightarrow B$ y $g : C \rightarrow D$ son inyectivas y si $A \cap C = \emptyset$ y $\mathcal{R}(f) \cap \mathcal{R}(g) = \emptyset$, entonces también $f \cup g : A \cup C \rightarrow B \cup D$ es inyectiva.*

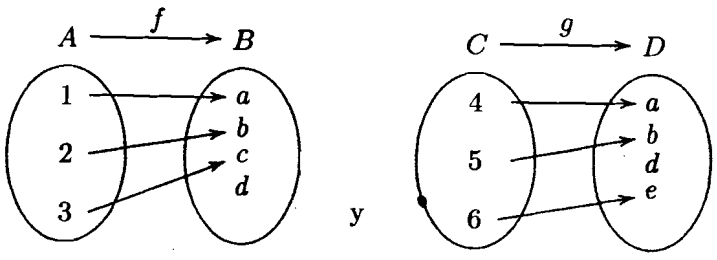
Demostración. Supongamos $(f \cup g)(u) = (f \cup g)(v)$.

a) Si $u \in A$, entonces $(f \cup g)(u) = f(u)$ y no se podrá tener $(f \cup g)(v) = g(v)$ ya que los recorridos de f y g son disyuntos, así que $(f \cup g)(v) = f(v)$ y la hipótesis se transforma en $f(u) = f(v)$ y siendo f uno a uno, $u = v$.

b) Análogamente, si $u \in C$ se tiene $(f \cup g)(u) = g(u)$ y se deduce que $(f \cup g)(v) = g(v)$, de donde $g(u) = g(v)$ y siendo g uno a uno, $u = v$.

□

Nota. La condición $\mathcal{R}(f) \cap \mathcal{R}(g) = \emptyset$ es también necesaria pues si no se cumple se podrían tener funciones inyectivas como las f y g de los diagramas que siguen, sin que $f \cup g = \{(1,a), (2,b), (3,c), (4,a), (5,b), (6,e)\}$ lo sea.



DEFINICIÓN 11. *Se dice que una función $f : A \to B$ es* **sobreyectiva** *si todos los elementos de su codominio son imágenes por f de elementos del dominio, es decir si $\mathcal{R}(f) = B$.*

En otra forma:

$$f : A \to B \quad \text{es sobreyectiva} \leftrightarrow (\forall y \in B)(\exists x \in A)(f(x) = y).$$

También se dice en este caso que f es una función de A *sobre* B.

Por ejemplo la función idéntica de cualquier conjunto es sobreyectiva; también lo es $g : [0, +\infty) \to [0, +\infty)$ definida por $g(x) = x^2$, ya que $0 = g(0)$ y dado cualquier real $y > 0$, su raíz cuadrada positiva existe y $g(\sqrt{y}) = y$. En cambio la aplicación $f(x) = x^2$ de $\mathbb{R}$ en $\mathbb{R}$ no es sobreyectiva, debido a que ningún real negativo es el cuadrado (es la imagen) de un número real.

Las funciones trigonométricas $\text{sen}, \cos : \mathbb{R} \to \mathbb{R}$ no son sobreyectivas ya que $\mathcal{R}(\text{sen}) = \mathcal{R}(\cos) = [-1, 1]$, así que cualquier real menor que -1 o mayor que 1 no es imagen por la función sen ni por cos de otro real, mientras que $\tan : (-\pi/2, \pi/2) \to \mathbb{R}$, sí es sobreyectiva (e inyectiva!).

Obsérvese que $f : A \to B$ es sobreyectiva si y sólo si $\mathcal{R}(f) = B$. Con respecto a las funciones $f \times g$ y $f \cup g$ definidas anteriormente se cumple que:

TEOREMA 9. *Si $f : A \to B$ y $g : C \to D$ son sobreyectivas, entonces $f \times g : A \times C \to B \times D$ también lo es.*

Demostración. Dada cualquier (u, v) en $B \times D$, necesariamente $u \in B$ y $v \in D$ y como f y g son sobreyectivas, existen $x \in A$ y $z \in C$ tales que $f(x) = u$ y $g(z) = v$, es decir $(f(x), g(z)) = (u, v)$ o sea que $(f \times g)(x, z) = (u, v)$, quedando demostrado. □

TEOREMA 10. *Si $f : A \to B$ y $g : C \to D$ son sobreyectivas, y $A \cap C = \emptyset$ entonces $f \cup g$ es una función de $A \cup C$* **sobre** *$B \cup D$.*

Demostración. Como $\mathcal{R}(f \cup g) = \mathcal{R}(f) \cup \mathcal{R}(g)$ y teniéndose $\mathcal{R}(f) = B$ y $\mathcal{R}(g) = D$ por ser f y g sobreyectivas, entonces $\mathcal{R}(f \cup g) = B \cup D$, quedando demostrado. □

DEFINICIÓN 12. *Se dice que una función $f : A \to B$ es* **biyectiva** (o que es una **biyección** *de A en B o que es una* **correspondencia biunívoca**) *si f es simultáneamente inyectiva y sobreyectiva.*

Teniendo en cuenta los ejemplos analizados, $g(x) = x^2$ de $[0, +\infty)$ en $[0, +\infty)$ y $tg : (-\pi/2, \pi/2) \to \mathbb{R}$ son biyectivas, lo mismo que la función idéntica $I_A : A \to A$. Además:

COROLARIO 1. *Si $f : A \to B$ y $g : C \to D$ son biyectivas, también lo es $f \times g : A \times C \to B \times D$.*

COROLARIO 2. *Si $f : A \to B$ y $g : C \to D$ son biyectivas y $A \cap C = \emptyset$ y $\mathcal{R}(f) \cap \mathcal{R}(g) = \emptyset$ entonces $f \cup g$ es una biyección de $A \cup C$ en $B \cup D$.*

Terminaremos esta sección con la definición de dos conceptos muy útiles posteriormente.

DEFINICIÓN 13. *Sea $f : A \to B$ y sea $M \subseteq A$; se llama* **imagen de** *M por f al conjunto de las imágenes por f de los elementos de M. Si lo notamos por $f(M)$, se tiene*

$$f(M) = \{f(x) \mid x \in M\}$$

o más formalmente:

$$f(M) = \{y \in B \mid (\exists x)(x \in M \wedge f(x) = y)\}.$$

Por ejemplo si $f : \mathbb{R} \to \mathbb{R}$ está dada por $x \mapsto x^2$ y $M = [-1, 2]$, entonces $f(M) = [0, 4]$, como puede comprobarlo el lector usando la gráfica de esta función.

Análogamente $sen([0, \pi]) = [0, 1]$ y $sen(\mathbb{R}) = [-1, 1]$.

DEFINICIÓN 14. *Sea $f : A \to B$ y sea $N \subseteq B$; se llama* **imagen recíproca de** *N por f al subconjunto de A constituido por todos aquellos elementos cuyas imágenes por f pertenecen a N; se nota por $f^{-1}(N)$.*

Más brevemente: $f^{-1}(N) = \{x \in A | f(x) \in N\}$

Por ejemplo si $f : \mathbb{R} \to \mathbb{R}$ está definida por $x \to x^2$, entonces

$f^{-1}([1,4]) = [-2,-1] \cup [1,2]$;

$sen^{-1}([0,1]) = [0,\pi] \cup [2\pi, 3\pi] \cup [-2\pi, -\pi] \cdots = \bigcup_{n\in\mathbb{Z}} [2n\pi, 2n\pi + \pi]$.

La imagen recíproca y la imagen (directa) poseen propiedades muy interesantes, algunas de las cuales se encuentran entre los ejercicios. A manera de ejemplo probaremos que $f(\bigcap_{M\in\mathfrak{C}} M) \subseteq \bigcap_{M\in\mathfrak{C}} f(M)$ cuando $\mathfrak{C}$ es una colección no vacía de subconjuntos de A y $f : A \to B$.

En efecto, si $y \in f(\bigcap_{M\in\mathfrak{C}} M)$, entonces y es imagen por f de algún elemento $x \in \bigcap_{M\in\mathfrak{C}} M$, es decir $(\exists x)(\forall M \in \mathfrak{C})(x \in M \wedge y = f(x))$ de donde, por el ejercicio 16. sección 3 del Capítulo I,
$(\forall M \in \mathfrak{C})(\exists x)(x \in M \wedge y = f(x))$, es decir $(\forall M \in \mathfrak{C})(y \in f(M))$ o sea $y \in \bigcap_{M\in\mathfrak{C}} f(M)$.

¿Cuándo se cumple la igualdad?

Probaremos que ésta se tiene cuando f es inyectiva; bastará demostrar que en este caso $\bigcap_{M\in\mathfrak{C}} f(M) \subseteq f(\bigcap_{M\in\mathfrak{C}} M)$. En efecto:

Si $y \in \bigcap_{M\in\mathfrak{C}} f(M)$, entonces $(\forall M \in \mathfrak{C})(y \in f(M))$, es decir en cada M existe un elemento x_M tal que $y = f(x_M)$. Pero siendo f inyectiva, todos los x_M deberán ser el mismo elemento, llamémoslo x, estará así en todos los M, luego $y = f(x)$ o sea $y \in f(\bigcap_{M\in\mathfrak{C}} M)$, quedando demostrado.

También es cierta una especie de recíproca: si $f : A \to B$ es cualquier función y $f(\bigcap_{M\in\mathfrak{C}} M) = \bigcap_{M\in\mathfrak{C}} f(M)$, para toda colección $\mathfrak{C}$ no vacía de subconjuntos de A, entonces f es inyectiva.

Podemos demostrar lo anterior en una forma más general, cuando la propiedad se cumple tan solo para colecciones $\mathfrak{C}$ con dos elementos:

$$\text{Si} \quad \forall M_1, M_2 \subseteq A, \qquad f(M_1) \cap f(M_2) = f(M_1 \cap M_2),$$

entonces f es inyectiva. En efecto:

Si $f(x_1) = f(x_2) = y$, entonces $f(\{x_1\}) = f(\{x_2\}) = \{y\}$ o sea

$$f(\{x_1\}) \cap f(\{x_2\}) = \{y\}$$

y teniendo en cuenta la hipótesis,

$$f(\{x_1\} \cap \{x_2\}) = \{y\}$$

En consecuencia $\{x_1\} \cap \{x_2\}$ no podrá ser vacío (puesto que y debe ser imagen de un elemento de dicha intersección); siendo unitarios los dos conjuntos, necesariamente deberán ser iguales, es decir, $x_1 = x_2$ probándose que f es inyectiva.

Ejercicios

1. ¿Puede usted, observando la gráfica de una relación, decir si es una función o no? ¿Y mirando el diagrama sagital? ¿Qué criterios emplea?

2. Dibuje el gráfico de una función constante de $\mathbb{R}$ en $\mathbb{R}$.

3. ¿Son las funciones *sen*, *cos* : $\mathbb{R} \to \mathbb{R}$ inyectivas? ¿Por qué?

4. Halle criterios para saber, observando sólo la gráfica o sólo el diagrama sagital de una función de A en B, a) si es inyectiva y b) si es sobreyectiva.

5. ¿Es $\emptyset \subseteq A \times B$ una función? ¿Es $\emptyset$ una función de A en B? ¿Por qué?

6. Sean $f : A \to B$ una función y M, M_1, M_2 subconjuntos de A. Pruebe que:

   (a) $M_1 \subseteq M_2 \to f(M_1) \subseteq f(M_2)$.

   (b) $f(M_1 \cup M_2) = f(M_1) \cup f(M_2)$.

   (c) $f(\bigcup_{M\in\mathfrak{C}} M) = \bigcup_{M\in\mathfrak{C}} f(M)$ siendo $\mathfrak{C}$ una colección no vacía de subconjuntos de $\mathfrak{C}$.

   (d) $(\forall M \in \mathcal{P}(A))(\forall x)(f(x) \in f(M) \leftrightarrow x \in M)$ si y sólo si f es inyectiva.

   (e) $(\forall M \in \mathcal{P}(A))[f(C_A M) \subseteq C_B f(M)]$ si y sólo si f es inyectiva.

   (f) $(\forall M \in \mathcal{P}(A))[C_B f(M) \subseteq f(C_A M)]$ si y sólo si f es sobreyectiva.

   (g) $(\forall M_1, M_2 \in \mathcal{P}(A))[f(M_1 - M_2) = f(M_1) - f(M_2)]$ si y sólo si f es inyectiva.

   (h) $(\forall M_1, M_2 \in \mathcal{P}(A))[M_1 \subseteq M_2 \leftrightarrow f(M_1) \subseteq f(M_2)]$ si y sólo si f es inyectiva.

7. Sean $f : A \to B$ una función, N, N_1, N_2 subconjuntos de B y M un subconjunto de A. Demuestre que:

   (a) $N_1 \subseteq N_2 \to f^{-1}(N_1) \subseteq f^{-1}(N_2)$.

(b) $f^{-1}(N_1 \cup N_2) = f^{-1}(N_1) \cup f^{-1}(N_2)$.

(c) $f^{-1}(\bigcup_{N\in\mathfrak{C}} N) = \bigcup_{N\in\mathfrak{C}} f^{-1}(N)$ siendo $\mathfrak{C}$ una colección de subconjuntos de B.

(d) $f^{-1}(N_1 \cap N_2) = f^{-1}(N_1) \cap f^{-1}(N_2)$.

(e) $f^{-1}(\bigcap_{N\in\mathfrak{C}} N) = \bigcap_{N\in\mathfrak{C}} f^{-1}(N)$ siendo $\mathfrak{C}$ una colección de subconjuntos de B.

(f) $f^{-1}(N_1 - N_2) = f^{-1}(N_1) - f^{-1}(N_2)$.

(g) $f^{-1}(C_B N) = C_A f^{-1}(N)$.

(h) $f(f^{-1}(N)) \subseteq N$.

(i) $(\forall N \in \mathcal{P}(B))[f(f^{-1}(N)) = N]$ si y sólo si f es sobreyectiva.

(j) $M \subseteq f^{-1}(f(M))$.

(k) $(\forall M \in \mathcal{P}(A))[M = f^{-1}(f(M))]$ si y sólo si f es inyectiva.

(l) $(\forall N_1, N_2 \in \mathcal{P}(B))[N_1 \subseteq N_2 \leftrightarrow f^{-1}(N_1) \subseteq f^{-1}(N_2)]$ si y sólo f es sobreyectiva.

(m) $f(M \cap f^{-1}(N)) = f(M) \cap N$.

8. Sea $f : A \to B$; definimos otra función

$$\hat{f} : \mathcal{P}(A) \to \mathcal{P}(B) \qquad \text{así:} \qquad \text{si} \qquad M \in \mathcal{P}(A),$$
$$\hat{f}(M) = \{f(x) | x \in M\}$$

Demuestre que:

a) $\hat{f}$ es uno a uno si y sólo si f es uno a uno.

b) f es sobreyectiva si y sólo si $\hat{f}$ es sobreyectiva.

+9. Muchas veces, cuando se está trabajando con funciones a valor real ($\mathbb{R}$ como codominio) definidas sobre subconjuntos de $\mathbb{R}$, tan solo se dice p.ej. "sea la función $y = \sqrt{x^2 - 5x + 6}$", sin especificar cuál es su dominio. Se considera en estos casos que el dominio de una función f es el "máximo" subconjunto de $\mathbb{R}$ que puede servir como tal. En el ejemplo anterior sería $\mathcal{D}(f) = \{x \in \mathbb{R} | x^2 - 5x + 6 \geq 0\}$ ya que $x^2 - 5x + 6$ debe ser positivo o cero para que su raíz cuadrada sea un real; resolviendo la inecuación, $\mathcal{D}(f) = (-\infty, 2] \cup [3, +\infty)$.

Halle el dominio de cada una de las siguientes funciones a valor real:

a) $f(x) = \sqrt{x^2 + x - 6}$.

b) $f(x) = \sqrt{x^2 + 5x + 6}$.

c) $f(x) = \sqrt[3]{x - 1}$.

d) $f(x) = \sqrt{x + 1}/(x + 1)$.

10. Si f y g son funciones, ¿es siempre $f \cap g$ una función? ¿y $f - g$?

+11. La resta entre enteros es una operación que a cada pareja m, n le hace corresponder otro entero $m - n$; como $m - n \neq n - m$, la pareja deberá ser ordenada, de manera que la resta es una función de $\mathbb{Z} \times \mathbb{Z}$ en $\mathbb{Z}$ que envía (m, n) en $m - n$. Generalizando:

Una *operación binaria* $*$ en un conjunto A, es una función

$$* : A \times A \to A$$
$$(x, y) \mapsto x * y$$

a) Decimos que $*$ es conmutativa si $\forall x, y \in A, \quad x * y = y * x$. Dé dos ejemplos de operaciones conmutativas y dos de operaciones que no lo sean.

b) La operación $*$ se llama asociativa si $\forall x, y, z \in A, (x * y) * z = x * (y * z)$. Halle dos operaciones asociativas y dos que no lo sean.

c) Se dice que $*$ es modulativa si existe un elemento e en A tal que $(\forall x \in A)(e * x = x = x * e)$. El elemento e se llama el módulo de la operación $*$.

Encuentre tres operaciones modulativas y dos que no lo sean.

d) Una operación modulativa (con módulo e) se llama invertiva si $(\forall x \in A)(\exists y \in A)(x * y = e = y * x)$.

Halle dos operaciones invertivas y dos modulativas no invertivas.

12. Sea $\mathfrak{F}$ una colección de funciones tales que sus dominios son disyuntos dos a dos. Pruebe que $\bigcup_{f\in\mathfrak{F}} f$ es una función de $\bigcup_{f\in\mathfrak{F}} \mathcal{D}(f)$ *sobre* $\bigcup_{f\in\mathfrak{F}} \mathcal{R}(\{)$.

+13. Sea $\mathfrak{F}$ una colección no vacía de biyecciones tales que sus dominios son disyuntos dos a dos y sus recorridos también son disyuntos dos a dos. Demuestre entonces que $\bigcup_{f\in\mathfrak{F}} f$ es una función biyectiva de $\bigcup_{f\in\mathfrak{F}} \mathcal{D}(f)$ sobre $\bigcup_{f\in\mathfrak{F}} \mathcal{R}(f)$.

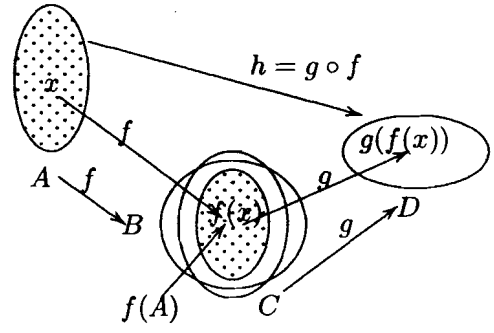
+14. Sea $\mathfrak{C}$ una colección de funciones tales que de dos cualesquiera de $\mathfrak{C}$, siempre una de ellas es una extensión de la otra, o sea que $(\forall f, g \in \mathfrak{C})(f \subseteq g \vee g \subseteq f)$.

a) Demuestre que $\bigcup_{f\in\mathfrak{F}} f$ es una función.

b) Si todas las funciones de $\mathfrak{C}$ son inyectivas, entonces $\bigcup_{f\in\mathfrak{F}} f$ también es inyectiva.

3.4 COMPOSICIÓN DE FUNCIONES

Sean $f : A \to B$ y $g : C \to D$ tales que $f(A) \subseteq C$. Es posible en este caso, a partir de las dos funciones anteriores, construir una tercera $h : A \to D$ en la forma siguiente:



Como para todo x de A su imagen $f(x)$ pertenece al dominio de g, es posible calcular la imagen por g de $f(x)$. Definimos entonces la función h mediante

$$h(x) = g(f(x)).$$

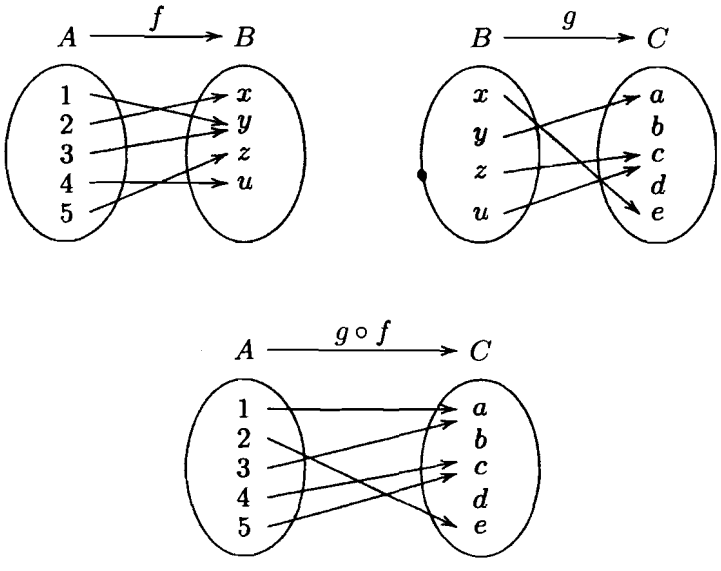
Es costumbre usar la notación $h = g \circ f$ (léase "efe compuesto ge") y decir que h es la *función compuesta de f y g*. Así,
$(\forall x \in A)[(g \circ f)(x) = g(f(x))]$.

Por ejemplo si $f = tg : (-\pi/2, \pi/2) \to \mathbb{R}$ y $g : \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$ es tal que $g(x) = x^2$, entonces $g \circ tg : (-\pi/2, \pi/2) \to \mathbb{R}^+ \cup \{0\}$ claramente está dada por $(g \circ tg)(x) = g(tg(x)) = (tg(x))^2 = tg^2 x$.

Nótese que en este caso no existe $tg \circ g$ ya que por ejemplo $tg(g(\sqrt{\pi/2}))$ no está definido por no pertenecer $g(\sqrt{\pi/2}) = \pi/2$ al dominio de tg.

Algo semejante sucede con la compuesta de las dos funciones dadas por sus diagramas sagitales en la figura que sigue adelante: $g \circ f$ existe pero no es posible formar $f \circ g$ ya que ningún elemento de $g(B)$ pertenece a $A = \mathcal{D}(f)$

Aún en casos como $f : \mathbb{R} \to \mathbb{R}$ y $g : \mathbb{R} \to \mathbb{R}$ dadas por $f(x) = x^2$ y $g(x) = x + 1$, en los cuales está definida tanto $g \circ f$ como $f \circ g$, generalmente



$g \circ f \neq f \circ g$; así para estas últimas funciones,

$$(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 1 \quad y$$

$$(f \circ g)(x) = f(g(x)) = f(x+1) = (x+1)^2 = x^2 + 2x + 1,$$

de modo que para todo x no nulo, $(g \circ f)(x) \neq (f \circ g)(x)$.

La composición de funciones es asociativa, ya que si se tienen por.ej. $f : A \to B$, $g : B \to C$, $h : C \to D$, tanto $h \circ (g \circ f)$ como $(h \circ g) \circ f$ poseen dominio A y codominio D y además, para todo x de A,

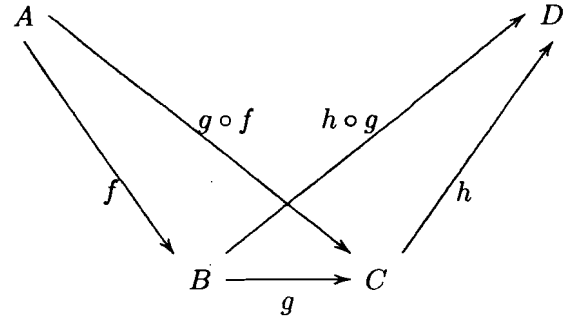
$$(h \circ (g \circ f))(x) = h((g \circ f)(x) = h(g(f(x)))$$

y

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))),$$

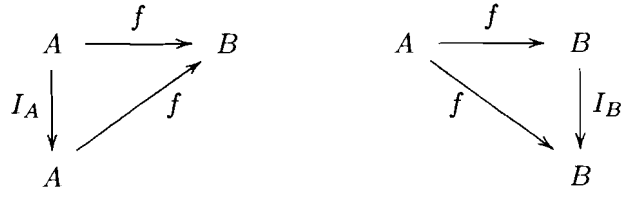
de modo que se tiene la igualdad.

Esta afirmación se hace algunas veces simplemente diciendo que el siguiente diagrama es conmutativo:



Debe entenderse que entre dos conjuntos cualesquiera siempre se obtiene el mismo resultado, sin importar el camino seguido; por ejemplo, entre A y D se puede tomar f y luego $h \circ g$ (es decir, $(h \circ g) \circ f$) o primero $g \circ f$ y luego h (o sea $h \circ (g \circ f)$; al final el efecto es el mismo.

También son conmutativos los diagramas



es decir, $f \circ I_A = f$ y $I_B \circ f = f$, lo cual significa que con respecto a la composición de funciones, la identidad del conjunto de partida (I_A) actúa como módulo a la derecha y la del conjunto de llegada I_B como módulo a la izquierda. Para verlo basta observar que cualquiera sea x en A,

$$(f \circ I_A)(x) = f(I_A(x)) = f(x)$$
$$(I_B \circ f)(x) = I_B(f(x)) = f(x).$$

Con respecto a los conceptos ya introducidos se tienen los resultados siguientes:

TEOREMA 11.

a) *La función compuesta de dos inyecciones es una inyección.*

b) *Si $f : A \to B$ y $g : B \to C$ son funciones sobreyectivas, entonces $g \circ f$ también es sobreyectiva.*

c) *Si* $f: A \to B$ *y* $g: B \to C$ *son biyecciones, entonces* $g \circ f$ *también lo es.*

Demostración.

a) Sean $f: A \to B$ y $g: C \to D$ tales que $f(A) \subseteq C$. Si f y g son inyectivas y $(g \circ f)(x_1) = (g \circ f)(x_2)$, se tiene que $g(f(x_1)) = g(f(x_2))$ y siendo g inyectiva, necesariamente $f(x_1) = f(x_2)$; el ser f inyectiva hace que $x_1 = x_2$, quedando demostrado.

b) Si f es sobreyectiva, entonces $f(A) = B$ y análogamente $g(B) = C$, luego $C = g(B) = g(f(A)) = (g \circ f)(A)$ lo cual significa que también $g \circ f$ es sobreyectiva.

La parte c) es un corolario inmediato de las dos anteriores. □

Aún debemos, con respecto a la composición de funciones, responder la pregunta siguiente:

Dada una función $f: A \to B$, ¿Cuándo existe otra $g: B \to A$ tal que $g \circ f = I_A$ y $f \circ g = I_B$?

Decir $g \circ f = I_A$ y $f \circ g = I_B$ significa que cualquiera sea x en A, $g(f(x)) = x$ y cualquiera sea y en B, $f(g(y)) = y$.

Obsérvese que el efecto producido por una de las funciones es siempre anulado por la otra.

Esto significa que si $y = f(x)$, entonces $g(y) = x$ y recíprocamente, es decir, $(x, y) \in f \leftrightarrow (y, x) \in g$, lo cual nos conduce a que necesariamente $g = f^{-1}$, la relación inversa de f.

Inmediatamente nos asalta la duda: ¿Es la relación f^{-1} realmente una función? ¡No siempre! Si existiesen dos elementos distintos x_1, x_2 de A tales que $(x_1, y) \in f$ y $(x_2, y) \in f$, entonces $(y, x_1) \in f^{-1}$ y $(y, x_2) \in f^{-1}$ y así f^{-1} no sería función. En consecuencia, la primera restricción que se debe imponer es que f debe ser inyectiva; en efecto:

TEOREMA 12. *Si* f *es una función inyectiva, entonces la* relación f^{-1} *es una función y también es inyectiva.*

Demostración. Si $(u, v) \in f^{-1} \wedge (u, z) \in f^{-1}$, entonces $(v, u) \in (f^{-1})^{-1} = f$ y $(z, u) \in f$ o sea $f(v) = u = f(z)$ y siendo f inyectiva se tendrá $v = z$, demostrándose que f^{-1} es función. Veamos que f^{-1} es inyectiva: si $f^{-1}(a) = f^{-1}(b) = y$, se tiene que $(a, y) \in f^{-1} \wedge (b, y) \in f^{-1}$ o sea $(y, a) \in f \wedge (y, b) \in f$ y siendo f función se tendrá $a = b$. □

Casi tenemos contestada la pregunta que nos hicimos; nos resta un detalle: si $f: A \to B$ es inyectiva, f^{-1} es una función pero $\mathcal{D}(f^{-1}) = \mathcal{R}(f)$ así que el dominio de f^{-1} será B si y sólo si f es sobreyectiva.

Observamos además que $\mathcal{R}(f^{-1}) = \mathcal{D}(f) = A$, así que f^{-1} también resulta ser sobreyectiva. Resumiendo:

TEOREMA 13. *Si* $f: A \to B$ *es una biyección, entonces existe otra biyección* $g: B \to A$ *tal que* $g \circ f = I_A$ *y* $f \circ g = I_B$*; además* $g = f^{-1}$.

Se dice en este caso que g *es la función inversa de* f y que f es la función inversa de g (ya que $f = (f^{-1})^{-1} = g^{-1}$) o que f y g son inversas.

El teorema anterior puede reformularse en esta terminología: Si f es una biyección de A en B, entonces f tiene una función inversa. Su recíproco también es cierto:

TEOREMA 14. *Si* $f: A \to B$ *tiene función inversa, entonces* f *es una biyección.*

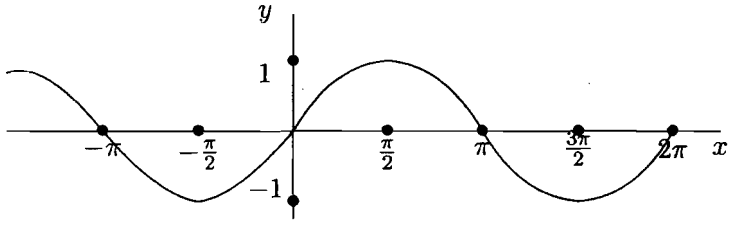
Demostración. Sea $f: A \to B$ y sea $g: B \to A$ su inversa. Si $f(x_1) = f(x_2)$, entonces $g(f(x_1)) = g(f(x_2))$ o sea $(g \circ f)(x_1) = (g \circ f)(x_2)$, es decir, $I_A(x_1) = I_A(x_2)$ o lo que es lo mismo $x_1 = x_2$, siendo f inyectiva. Sea y cualquier elemento de B. $y = I_B(y) = (f \circ g)(y) = f(g(y))$, así que y es la imagen por f de $x = g(y)$, siendo f sobreyectiva. □

Juntando los dos últimos teoremas se obtiene:

COROLARIO 1. *Una función* $f: A \to B$ *posee función inversa si y sólo si es una biyección.*

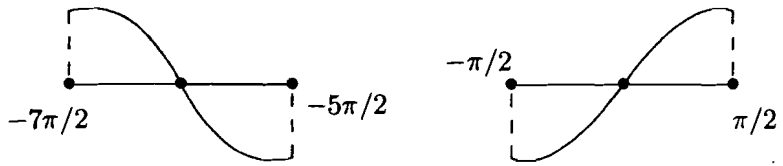
Con esto queda completamente respondida nuestra pregunta inicial.

Algunas veces es necesario disponer de funciones inversas de otras dadas; por ejemplo, todos hemos trabajado con la función arcsen, supuestamente "inversa" de la función sen; pero según el corolario anterior sen: $\mathbb{R} \to \mathbb{R}$ no puede tener función inversa ya que no es inyectiva ni sobreyectiva.



y =sen x

¿Qué es lo que realmente sucede?
Generalmente el punto de la curva donde se necesita usar la inversa puede localizarse, es decir, no es necesario considerar "toda" la función sino solamente una parte de ella, una porción de la función (o una *restricción*, como se le acostumbra llamar) que sea biyectiva y luego sí se halla la inversa de dicha porción. Por ejemplo, gráficamente y con respecto a la función *sen*, las partes



se pueden interpretar como gráficas de biyecciones, la primera de $[-7\pi/2, -5\pi/2]$ en $[-1,1]$ y la segunda de $[-\pi/2, \pi/2]$ en $[-1,1]$.

DEFINICIÓN 15. *Se dice que una función g es una restrición de otra función f, si $g \subseteq f$. También se dice en este caso que f es una extensión de g.*

Obsérvese que $((x.y) \in g) \rightarrow ((x,y) \in f)$ significa que $(y = g(x))$ implica $(y = f(x))$ es decir, $(\forall x \in \mathcal{D})(g(x) = f(x))$. Por esto, cuando se consideran funciones entre conjuntos, se acostumbra decir que es una extensión de $g : C \rightarrow D$ es otra función $f : A \rightarrow B$ tal que $A \supseteq C$, $B \supseteq D$ y $\forall x \in C$, $f(x) = g(x)$.

Análogamente se dice que $g : C \rightarrow D$ es una restricción de la función $f : A \rightarrow B$. Cuando se deja el mismo codominio, se acostumbra usar la notación $f\restriction_C : C \rightarrow B$ y se lee "la restricción de f a C".

Por ejemplo, una restricción de $f : \mathbb{R} \rightarrow \mathbb{R}$ dada por $f(x) = |x|$ (función valor absoluto) es $f_{|\mathbb{R}^+} : \mathbb{R}^+ \rightarrow \mathbb{R}$, la cual resulta ser una inyección canónica: $f_{|\mathbb{R}^+}(x) = |x| = x$ ya que $x > 0$.

Extensiones de $g : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ dada por $g(x) = x$ son $f : \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) = \frac{x+|x|}{2}$ y $h : \mathbb{R} \rightarrow \mathbb{R}$ dada por $h(x) = |x|$. como puede comprobarlo fácilmente el lector.

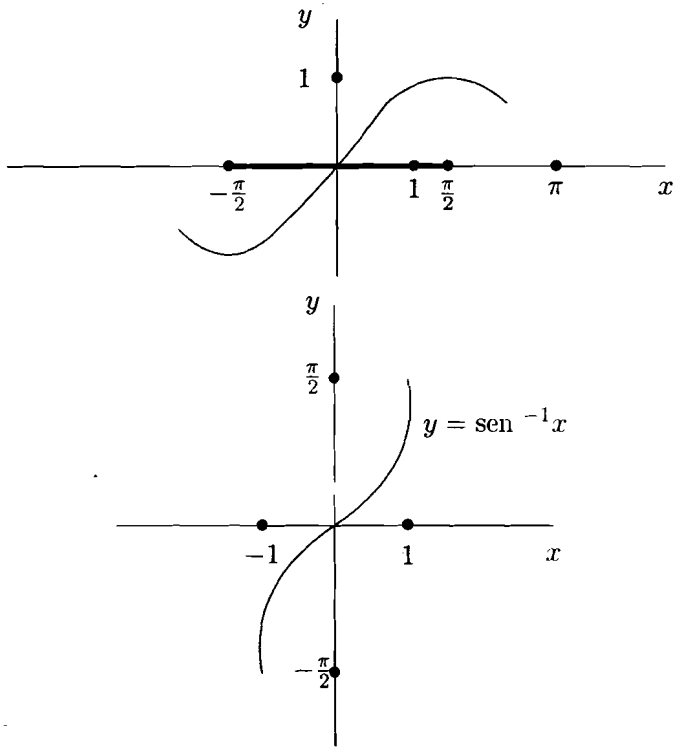
Fijemos nuevamente nuestra atención en el problema de las funciones inversas; puede enunciarse en la forma: *dada una función $f : A \rightarrow B$, hallar una de sus restricciones que sea biyectiva maximal y encontrar la función inversa de esta restricción.*

Teóricamente es muy fácil volver sobreyectiva a cualquier función dada

$f : A \rightarrow B$; basta (p.ej.) tomar como codominio su mismo recorrido:

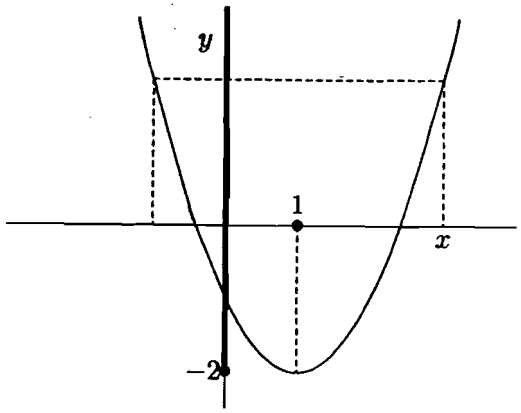
$f : A \rightarrow \mathcal{R}(f)$ es ya sobreyectiva y f no ha perdido aún ninguna de sus parejas ordenadas. A continuación, variando solamente f y A, debemos hallar una restricción $f\restriction_C : C \rightarrow \mathcal{R}(f)$ biyectiva, es decir, debemos conseguir una función inyectiva f_1 con $f_1 \subseteq f$, tal que $\mathcal{R}(f_1) = \mathcal{R}(f)$ y así se tiene que $f_1 : C \rightarrow \mathcal{R}(f)$ será la biyección deseada y tendrá inversa $f_1^{-1} : \mathcal{R}(f) \rightarrow C$.

Con respecto a $sen : \mathbb{R} \rightarrow \mathbb{R}$, se tendría $sen : \mathbb{R} \rightarrow [-1,1]$ sobreyectiva y restricciones biyectivas serían entre otras,
$sen_1 : [-7\pi/2, -5\pi/2] \rightarrow [-1,1]$ y $sen_2 : [-\pi/2, \pi/2] \rightarrow [-1,1]$; no lo sería $sen_3 : [0,\pi] \rightarrow [-1,1]$ porque dejaría de ser sobreyectiva. Es práctica común trabajar con $sen_2 : [-\pi/2, \pi/2] \rightarrow [-1,1]$ y llamar *Arc Sen* a su función inversa: $Arc\,Sen : [-1,1] \rightarrow [-\pi/2, \pi/2]$ tal que $y \mapsto Arc\,Sen\,y$.

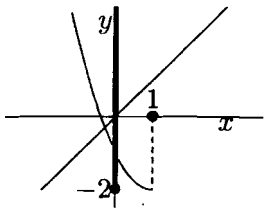


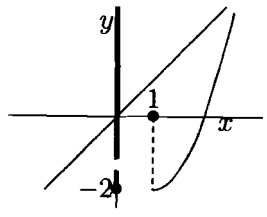
Repitamos el procedimiento en otro caso particular: sea $f : \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) = x^2 - 2x - 1$. Sabemos que la gráfica de $y = x^2 - 2x - 1$ es una parábola que abre hacia arriba, de modo que la búsqueda del recorrido de f se reduce a hallar el punto más bajo de la parábola, el valor mínimo tomado por la función, ya sea usando técnicas del cálculo diferencial o con una adecuada descomposición; preferimos esta última: $y = x^2 - 2x - 1 = x^2 - 2x + 1 - 2 = (x-1)^2 - 2$.

Siendo $(x-1)^2 \geq 0$, el mínimo valor de y se obtiene cuando es cero: $(x-1)^2 = 0$, es decir cuando $x = 1$ y valdrá $y = -2$



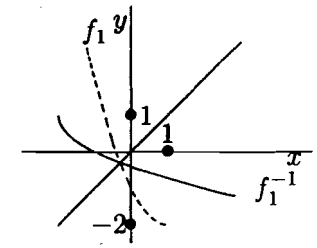
Así la función $f: \mathbb{R} \to [-2, +\infty)$ es sobreyectiva. Restricciones biyectivas se pueden tener de muchas maneras, pero si se quiere seguir conservando la continuidad y la derivabilidad de la función en todos sus puntos, sólo tenemos dos posibilidades:





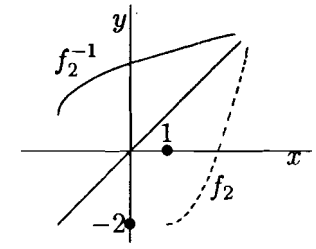
$$f_1 : (-\infty, 1] \to [-2, +\infty) \qquad \text{y} \qquad f_2 : [1, \infty) \to [-2, \infty)$$
$$x \mapsto x^2 - 2x + 1 \qquad\qquad x \mapsto x^2 - 2x - 1$$

Si se quieren dibujar directamente sus inversas f_1^{-1} y f_2^{-1}, como éstas se obtienen con solo intercambiar las componentes de sus parejas ordenadas, gráficamente el punto (y, x) es el simétrico de (x, y) de modo que bastará reflejar con respecto a la recta $y = x$ dichas gráficas.



$$f_1^{-1} : [-2, +\infty) \to (-\infty, 1]$$

y



$$f_2^{-1} : [-2, +\infty) \to [1, -\infty)$$

Algebraicamente las inversas se hallan siguiendo la misma idea: intercambiar x con y y luego "despejar" y para tener la inversa como función de x, de manera que sus gráficas sean precisamente las dos anteriores.

Procedamos: en $y = x^2 - 2x - 1$ intercambiemos x con y

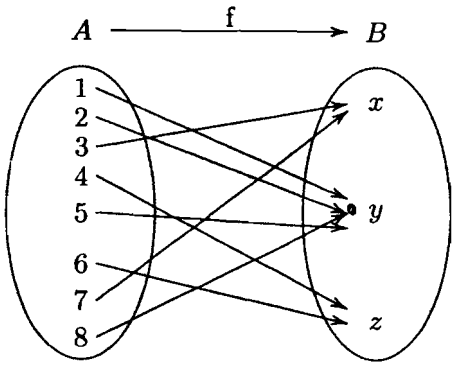
$$x = y^2 - 2y - 1$$

Despejemos y: $0 = y^2 - 2y - (1 + x)$ es una ecuación de segundo grado en y de la forma $0 = ay^2 + by + c$, luego

$$y = \frac{2 \pm \sqrt{4 + 4(1+x)}}{2} = 1 \pm \sqrt{1 + (1+x)}\,.$$

Estando la gráfica de f_1^{-1} por debajo de la recta $y = 1$, su expresión se obtendrá tomando el signo "$-$" en la fórmula anterior: $f_1^{-1}(x) = 1 - \sqrt{2+x}$. Análogamente $f_2^{-1}(x) = 1 + \sqrt{2+x}$, observándose que x deberá ser mayor o igual que -2, precisamente el dominio precalculado.

Consideremos un último ejemplo; dada la sobreyección del diagrama, hallar una restricción biyectiva $g: C \to B$



Intuitivamente lo único que se debe hacer es eliminar, junto con sus elementos de partida, algunas flechas que están de más.

Por ejemplo, al elemento x llegan flechas de 3 y 7, es decir $\{(3,x),\ (7,x)\}$ es el conjunto de las parejas de f que poseen x como segunda componente; de dicho conjunto debemos escoger una de las dos parejas ordenadas, digamos $(3,x)$.

Análogamente $\{(1,y),(2,y),(5,y),(8,y)\}$ es el subconjunto de f constituido por las parejas con y como segunda componente y de él debemos elegir una única pareja; sea ésta $(5,y)$.

Finalmente de $\{(4,z),(6,z)\}$ elegimos $(6,z)$; obtenemos así la función $g = \{(3,x),\ (5,y),(6,z)\}$ que es la restricción biyectiva buscada, con dominio $C = \{3,5,6\}$.

¿Qué sucede si el conjunto B posee infinitos elementos? Nunca terminaríamos de elegir de cada uno de los conjuntos $\{(x,y) \in f \mid y = u\}$ una única pareja ordenada para formar la restricción biyectiva deseada.

Se pone de presente que la construcción de la restricción biyectiva anterior, en el caso general, es imposible de lograr en este momento; se hace necesaria una nueva y poderosa herramienta que nos permita, dada cualquier colección de conjuntos no vacíos, elegir *simultáneamente* un elemento de cada conjunto; es el axioma llamado de elección.

Ejercicios

1. Pruebe que una restricción de una función $f : A \to B$ se puede definir simplemente como una función $g : C \to D$ tal que $g \subseteq f$ y $D \subseteq B$.

*2. Sea A un conjunto cualquiera no vacío y sea F el conjunto de todas las biyecciones de A en A. Demuestre que si se considera F provisto de la composición de funciones como operación, es un grupo.

3. (a) Si A es un conjunto con diez elementos y B otro con un único elemento, halle todas las funciones de A en B.

   (b) Halle todas las funciones de un conjunto A con tres elementos en otro B con dos elementos.

   (c) Halle todas las funciones de un conjunto A con cuatro elementos en otro B con dos elementos.

   (d) ¿Podría hallar una fórmula para calcular el número de funciones de un conjunto A con n elementos en otro B con m elementos? Podría justificar dicha fórmula?

4. Dada la función $f(x) = x^2 + 2x - 8$ de $\mathbb{R}$ en $\mathbb{R}$,

   (a) Halle su recorrido.

   (b) Restrinja el codominio de f para obtener una función sobreyectiva.

   (c) Sin variar el codominio de la función en b), halle una restricción biyectiva que sea continua.

   (d) Halle gráfica y algebraicamente la función inversa de la biyección hallada en c).

5. Si $f : A \to B$ y $g : B \to D$ son biyecciones, demuestre que la función inversa de $g \circ f$ es $f^{-1} \circ g^{-1}$.

6. Sea $\mathcal{C}$ una colección de funciones tal que:

$$(\forall f, g \in \mathcal{C})(\mathcal{D}(f) \cap \mathcal{D}(g) = D \neq \emptyset \to f \restriction D = g \restriction D).$$

   Pruebe que $\bigcup_{f \in \mathcal{C}} f$ es una función de $\bigcup_{f \in \mathcal{C}} \mathcal{D}(f)$ sobre $\bigcup_{f \in \mathcal{C}} \mathcal{R}(f)$.

3.5 PROPIEDADES DE LAS RELACIONES

En lo que sigue del capítulo sólo consideraremos relaciones definidas en un conjunto A (es decir de A en A). Comenzaremos dando algunos ejemplos de ellas y luego analizaremos, de cierta propiedades usuales, cuáles poseen y cuáles no. Emplearemos muchas veces la notación xRy en vez de $(x,y) \in R$.

Ejemplos de relaciones definidas en un conjunto:

1. Sea $A = \{a,b,c\}$; las siguientes (entre otras) son relaciones en A:

$$R_1 = \{(a,b),(a,a),(b,c),(c,b)\}$$
$$R_2 = \{(a,a),(a,b),(b,b),(c,c)\}$$
$$R_3 = \{(a,a),(a,b),(b,a),(b,b),(c,c)\}$$

2. Si A es cualquier conjunto, la igualdad entre elementos de A es una relación en A. Si se quiere expresar como conjunto de parejas ordenadas, ella sería

$$\triangle = \{(x,y) \in A \times A \mid x = y\}$$

Muchas veces se le acostumbra llamar "la diagonal de A" (represéntela gráficamente y hallará el motivo) y no es otra cosa que la función idéntica de A.

3. Si X es cualquier conjunto, la contenencia ("ser un subconjunto de") es una relación en $\mathcal{P}(X)$. Como conjunto de parejas, sería

$$\{(M,N) \in \mathcal{P}(X) \times \mathcal{P}(X) \mid M \subseteq N\}$$

Es un ejercicio para el lector formar este conjunto de parejas ordenadas para el caso $X = \{a,b,c\}$.

4. La relación de orden usual entre números naturales

$$\{(m,n) \in \mathbb{N} \times \mathbb{N} \mid m \leq n\}$$

5. Sea A un conjunto específico de personas; en él consideremos la relación "x posee el mismo padre o la misma madre que y".
Nota: El "o" usado es inclusivo.

6. Entre elementos del conjunto $\mathbb{Z}$ de los enteros definimos la relación "$a \equiv b(3)$" (léase "a es congruente con b módulo tres"), la cual significa "$a-b$ es múltiplo de 3". Por ejemplo $14 \equiv 2(3)$ ya que $14-2 = 12$ es un múltiplo de 3 y $5 \equiv 20(3)$ puesto que $5-20 = -15 = 3 \cdot (-5)$ también es múltiplo de 3. En resumen:

$$a \equiv b(3) \Leftrightarrow (\exists k \in \mathbb{Z})(a-b = 3k).$$

7. Generalizando el ejemplo anterior, sea m un entero fijo mayor que 1; definimos en $\mathbb{Z}$ la relación

$$a \equiv b(m) \Leftrightarrow (\exists k \in \mathbb{Z})(a-b = mk)$$

es decir, a es congruente con b módulo m si y sólo si $a-b$ es múltiplo de m, o lo que es lo mismo, si y sólo si $a-b$ es divisible (exactamente) por m.

8. Consideremos en $\mathbb{N} - \{0\} = \{1,2,3,4,5,...\}$ la relación "m es divisor de n". La simbolizaremos "mDn" y también la leeremos "m divide a n".

$$mDn \Leftrightarrow (\exists q \in \mathbb{Z})(n = mq)$$

o sea: m es divisor de n si n (dividendo) es igual a m (divisor) multiplicado por q (cociente).

9. Sea α un plano (fijo) y sea A el conjunto de todas las rectas contenidas en α. Consideremos en A la relación de paralelismo:

$$l \| r \Leftrightarrow (l = r \vee (l \cap r = \emptyset)).$$

Es decir, l es paralela a r si la distancia de los puntos de una de las rectas a la otra es constante (puede ser cero en el caso $l = r$).

10. Sea X un conjunto; la relación siguiente entre subconjuntos de X, es una relación en $\mathcal{P}(X)$:

$$M \approx N \Leftrightarrow (\exists f)(f : M \to N \wedge (f \text{ es biyectiva})).$$

Es decir $M \approx N$ (léase "M *es equipotente* con N") si y sólo existe una biyección de M sobre N.

Intuitivamente, si el lector se da ejemplos de la relación anterior entre subconjuntos de un conjunto X finito, hallará que $M \approx N$ significa que M tiene el mismo número de elementos que N.

DEFINICIÓN 16. *Una relación definida en A se llama* `reflexiva` *en A, si todo elemento de A está relacionado mediante ella consigo mismo.*

En el lenguaje objeto:

$$R \quad \text{es reflexiva en } A \Leftrightarrow (\forall x \in A)(xRx)$$

Las relaciones R_2 y R_3 del ejemplo 1. los son, lo mismo que la igualdad y la contenencia ya que $(\forall X \in A)(X = X)$ y $(\forall M \in \mathcal{P}(X))(M \subseteq M)$ respectivamente.

Puesto que"$(\forall m \in \mathbb{N})(m \leq m)$" y " x posee el mismo padre o la misma madre que x" son ciertas, también las relaciones de los ejemplos 4. y 5. son reflexivas.

Como $(\forall a \in \mathbb{Z})(a - a = m \cdot 0)$, entonces $(\forall a \in \mathbb{Z})(a \equiv a(m))$, siendo reflexiva la relación de congruencia módulo m entre enteros, y en consecuencia también la del ejemplo 6. .

Trivialmente $m = m \cdot 1$, así que todo número natural mayor que cero es divisor de sí mismo, luego la relación del ejemplo 8. también es reflexiva.

Según nuestra definición dada en 9., toda recta es paralela a sí misma, de modo que también esta relación es reflexiva.

Es posible construir varias biyecciones de un conjunto M en sí mismo, pero la más sencilla es la identidad de M, $I_M : M \to M$, luego $M \approx M$ siendo la relación en 10. también reflexiva.

No todas las relaciones son reflexivas claro está; por ejemplo "$x < y$" entre reales, "x es hijo de y" entre personas o la relación R_1 dada en 1., no lo son.

DEFINICIÓN 17. *Una relación definida en un conjunto se llama* `simétrica` *en dicho conjunto si cada vez que un elemento está relacionado (mediante ella) con otro, también el segundo lo está con el primero.*

$$R \quad \text{es simétrica en } A \Leftrightarrow (\forall x, y \in A)(xRy \to yRx)$$

En 1 es simétrica R_3 pero no lo son R_1 ni R_2 ya que en ambos casos a está relacionado con b pero b no lo está con a.

Como $(\forall x, y \in A)(x = y \to y = x)$, la igualdad en A es simétrica. La contenencia no lo es cuando el conjunto X no es vacío, ya que en este caso $\emptyset \subseteq X \wedge \neg(X \subseteq \emptyset)$.

Las relaciones de los ejemplos 4. y 8. no son simétricas ya que entre otros casos, en particular $2 \leq 3 \wedge \neg(3 \leq 2)$ y además $2D6 \wedge \neg(6D2)$.

Note que siendo $p \wedge (\neg q)$ la negación de $p \to q$, entonces R no es simétrica en A significa "$(\exists x, y \in A)(xRy \wedge \neg(yRx))$".

Trivialmente la relación en 5. es simétrica: si x posee el mismo padre o la misma madre que y, entonces y posee el mismo padre o la misma madre que x.

Si $a \equiv b(m)$, entonces existe k entero tal que $a - b = mk$ así que $b - a = m(-k)$ y siendo $-k$ entero, se concluye que $b \equiv a(m)$, obteniéndose la simetría.

Evidentemente entre rectas $l \| r \to r \| l$ de modo que la relación en 9. es simétrica. También lo es la equipotencia entre conjuntos dada en 10. Si $M \approx N$, existe $f : M \to N$ biyectiva y según el teorema 13 de la sección anterior, existe $f^{-1} : N \to M$ también biyectiva, luego $N \approx M$.

DEFINICIÓN 18. *Una relación R definida en A se llama* `antisimétrica` *en A si y sólo si cuando $x \neq y$, no se puede tener simultáneamente xRy y yRx.*

Así R es antisimétrica en A si y sólo si

$$(\forall x, y \in A)(x \neq y \to \neg(xRy \wedge yRx)).$$

Esto significa que si $x \neq y$, se puede tener:

$$\begin{array}{llll} xRy & \text{y no} & yRx & \text{o bien} \\ yRx & \text{y no} & xRy & \text{o bien} \\ & \text{no} & xRy & \text{y no} \quad yRx \end{array}$$

Así en el ejemplo 1. la relación R_2 es antisimétrica: Las parejas de elementos distintos son $a \neq b, a \neq c$ y $b \neq c$. En el primer caso se tiene que $aR_2b \wedge \neg(bR_2a)$; en los otros casos $(a, c) \notin R_2 \wedge (c, a) \notin R_2$ y también $(b.c) \notin R_2 \wedge (c, b) \notin R_2$.

En realidad está por demás verificar aquí para $a \neq c$ y $b \neq c$; basta comprobar que si una pareja (x, y) con $x \neq y$ está en la relación, no lo esté (y, x).

R_1 no es antisimétrica pues $b \neq c$ y sin embargo $(b, c) \in R_1 \wedge (c, b) \in R_1$; tampoco R_3 lo es porque $a \neq b$ y $(a, b) \in R_3 \wedge (b, a) \in R_3$.

La igualdad es una relación antisimétrica porque no existen parejas distintas que incumplan la condición de la definición, es decir, si $x \neq y$, ni x está relacionado con y mediante la igualdad, ni y lo está con x, así que trivialmente para x, y cualesquiera en A es cierta implicación

$$x \neq y \to \neg(x = y \wedge y = x).$$

Antes habíamos visto que la igualdad en A también era simétrica, de modo que antisimétrica *no* es la negación de simétrica; a la negación de simetría se le acostumbra llamar *asimetría.*

Debido a la equivalencia entre $p \to q$ y $\neg q \to \neg p$, algunas veces es útil reemplazar $x \neq y \to \neg(xRy \wedge yRx)$ por $xRy \wedge yRx \to x = y$ en la definición de antisimetría, obteniéndose la forma equivalente:

$$R \quad \text{es antisimétrica en } A \Leftrightarrow (\forall x, y \in A)(xRy \wedge yRx \to x = y)$$

Por ejemplo, $(\forall M, N \in \mathcal{P}(X))((M \subseteq N \wedge N \subseteq M) \to M = N)$ de modo que la contenencia es antisimétrica.

Análogamente el orden usual de naturales es antisimétrico:

$$(\forall m, n \in \mathbb{N})[(m \leq n) \wedge (n \leq m) \to m = n].$$

La relación del ejemplo 5. puede no ser simétrica: Si en el conjunto A existen *dos* hermanos X y Y, entonces $X \neq Y$ y "X posee el mismo padre o la misma madre que Y" y "Y posee el mismo padre o la misma madre que X" son verdaderas.

Las relaciones en 6. y 7. tampoco son antisimétricas ya que por ejemplo $13 \neq 4$ y $13 \equiv 4(3) \wedge 4 \equiv 13(3)$; también $1 \neq m+1$ y $1 \equiv m+1(m)$ y $m+1 \equiv 1(m)$.

En 8. "ser divisor de" es antisimétrica: Supongamos $mDn \wedge nDm$; existen entonces enteros p, q tales que $(n = mq) \wedge (m = np)$; reemplazando la segunda igualdad en la primera, $n = (np)q$; asociando adecuadamente y cancelando $n\,(\neq 0)$, $1 = pq$ y siendo p, q enteros, necesariamente $p = 1 = q$ ó $p = -1 = q$. la segunda posibilidad no puede tenerse debido a que $A = \{1, 2, 3, ...\}$ es un conjunto de enteros positivos, así que $p = 1 = q$, luego $n = mq = n \cdot 1 = m$, quedando demostrado.

El paralelismo entre rectas de un plano no es antisimétrico ya que se pueden tener rectas distintas l, m tales que $l \| m \wedge m \| l$.

La equipotencia entre subconjuntos de un conjunto dado X tampoco es antisimétrica en general, puesto que si X posee dos o más elementos, digamos $a \neq b$, entonces $\{a\} \neq \{b\}$ y $\{a\} \approx \{b\}$ y $\{b\} \approx \{a\}$ mediante las biyecciones únicas existentes.

DEFINICIÓN 19. *Una relación definida en un conjunto se llama* `transitiva` *en dicho conjunto, si cada vez que un elemento esté relacionado mediante ella con un segundo y éste a su vez lo esté con un tercero, entonces también el primero está relacionado con el tercero; más precisamente,*

$$R \quad \text{es transitiva en } A \Leftrightarrow (\forall x, y, z \in A)(xRy \wedge yRz \to xRz).$$

Por ejemplo las relaciones R_2 y R_3 dadas en 1. son transitivas, mientras que R_1 no lo es debido a que $(a, b) \in R_1$ y $(b, c) \in R_1$ pero $(a, c) \notin R_1$.

Como $(a = b) \wedge (b = c) \to a = c$ y $(M \subseteq N \wedge N \subseteq P) \to M \subseteq P$, tanto la igualdad como la contenencia son transitivas; evidentemente lo es la relación "$\leq$" entre números naturales.

La relación dada en 5. no es general transitiva, ya que puede suceder que x sea hermano medio de y, y sea hermano medio de z y x y z no sean hermanos medios, si la situación que se presenta es la siguiente:

x es hijo de P_1 y M_1; y es hijo de P_2 y M_1; z es hijo de P_2 y M_2, siendo los padres $P_1 \neq P_2$ y las madres $M_1 \neq M_2$.

La relación de congruencia módulo m es transitiva en $\mathbb{Z}$: si $a \equiv b(m)$ y $b \equiv c(m)$, existen $p, q \in \mathbb{Z}$ tales que $a - b = pm$ y $b - c = qm$; sumando miembro a miembro estas dos igualdades, $(a-b)+(b-c) = a-c = (p+q)m$ y siendo $p+q$ entero, se concluye que $a \equiv c(m)$.

Es muy sencillo ver que "m divide a n" en 8. y "$l \| r$" en 9. son relaciones transitivas. Finalmente, la equipotencia entre conjuntos definida en 10. también es transitiva: Si $M \approx N \wedge N \approx P$, entonces existen biyecciones $f : M \to N$ y $g : N \to P$; por la parte c) del teorema 11 de la sección 4 anterior, también es una biyección la compuesta $g \circ f : M \to P$, luego $M \approx P$.

Ejercicios

1. Si se considera $\emptyset$ como relación de A en A, ¿es reflexiva? ¿es simétrica? ¿es antisimétrica? ¿es transitiva?

2. Halle todas las relaciones definidas en el conjunto $A = \{a, b\}$.

3. Si A es un conjunto con n elementos, ¿podría hallar una fórmula que nos proporcione el número total de relaciones definidas en A?

4. Muestre que una relación R definida en A,

   (a) Es simétrica en A si y sólo si $R = R^{-1}$.

   (b) Es antisimétrica si y sólo si $R \cap R^{-1} \subseteq \triangle_A$.

5. De cada una de las relaciones siguientes, diga cuáles de las propiedades reflexiva, simétrica, antisimétrica y transitiva posee. Dé las razones de sus respuesta.

   a) $C \subseteq \mathbb{R} \times \mathbb{R}$ dada por $xCy \leftrightarrow cos\ (x-y) = 1$.

   b) $S \subseteq \mathbb{R} \times \mathbb{R}$ dada por $xSy \leftrightarrow sen(x-y) = 0$.

   c) $E \subseteq \mathbb{R} \times \mathbb{R}$ dada por $xEy \leftrightarrow x - y$ es un entero.

   d) $F \subseteq \mathbb{R}^2 \times \mathbb{R}^2$ dada por $(x,y)F(u,v) \leftrightarrow x^2 + y^2 \leq u^2 + v^2$.

   e) $R = \{(a,c),(a,a),(c,c),(b,c),(d,d),(c,a)\}$ definida en $A = \{a,b,c,d\}$.

6. Si se define la *"composición de relaciones"* R y S en la forma

$$S \circ R = \{(x,z)|(\exists y)((x,y) \in R \wedge (y,z) \in S)\},$$

   demostrar que una relación R definida en A es transitiva si y sólo si $R \circ R \subseteq R$.

7. Dé un ejemplo de una relación que no sea simétrica ni antisimétrica.

8. Pruebe que si una relación en A es simultáneamente simétrica, antisimétrica y reflexiva en A, entonces es la relación de igualdad en A.

9. ¿Será cierto que si Y posee n elementos, entonces el conjunto $\{(M,N) \in Y \times Y | M \subseteq N\}$ posee 3^n elementos?

   Dé la razón de su respuesta.

3.6 RELACIONES DE EQUIVALENCIA

Las propiedades más características de la igualdad son las reflexividad, la simetría y la transitividad. Una relación definida en un conjunto A que posea estas mismas tres propiedades, se comporta desde un cierto punto de vista, de manera semejante a la igualdad. Por ejemplo, la relación de paralelismo entre las rectas de un mismo plano es reflexiva, simétrica y transitiva; uno observa que todas las rectas paralelas poseen la misma dirección, así que para alguien interesado solamente en el aspecto "dirección", dos rectas paralelas son prácticamente indistinguibles.

DEFINICIÓN 20. *Una relación se llama de equivalencia en un conjunto A si ella es reflexiva, simétrica y transitiva en A.*

Según lo visto, las relaciones en 10. , 7. , 6. y la R_3 de 1. en la sección 5, son de equivalencia.

De las relaciones anteriores consideremos $a \equiv b(3)$ en $\mathbb{Z}$. Tomemos un entero cualquiera, por ejemplo 5, y encontremos el conjunto de todos aquellos enteros congruentes con 5 módulo 3:

$$\{..., -7, -4, -1, 2, \mathbf{5}, 8, 11, 14, ...\}$$

Elijamos ahora un entero que no esté en el conjunto hallado, p.ej. 10, y también formemos la colección de los enteros relacionados con 10 mediante la congruencia módulo 3:

$$\{..., -8, -5, -2, 1, 4, 7, \mathbf{10}, 13, 16, 19, ...\}$$

Tomemos otro entero que no pertenezca a los dos conjunto anteriores, digamos -6, y hallemos el conjunto (notado $[-6]$) de todos los enteros congruentes módulo 3 con -6:

$$[-6] = \{..., -12, -9, \mathbf{-6}, -3, 0, 3, 6, 9, 12, ...\}$$

En este momento el proceso anterior termina porque hemos agotado todos los enteros; usando notaciones análogas a $[-6]$, se tiene entonces que

$$[5] \cup [10] \cup [-6] = \mathbb{Z}.$$

Observamos además que los conjuntos $[5]$, $[10]$ y $[-6]$ son disyuntos dos a dos y que ninguno de ellos es vacío.

Escojamos en el conjunto [5] dos elementos cualesquiera, por ejemplo -4 y 11 y hallemos $[-4]$ y $[11]$. Nos encontramos sorpresivamente con que

$$[-4] = [5] = [11].$$

¿Es esta una propiedad general? ¿Lo son también las anteriores? Las respuestas son afirmativas.

DEFINICIÓN 21. *Sea R una relación de equivalencia definida en un conjunto A no vacío y sea b un elemento cualquiera de A; se llama* **clase de equivalencia de** b (con respecto a la relación R) *al conjunto constituido por todos los elementos de A que están relacionados mediante R con b.*

Se nota $[b]_R$ o simplemente $[b]$ si no hay lugar a confusiones.

Por ejemplo, si se considera en $\mathbb{Z}$ la relación de congruencia módulo 6,

$$\begin{aligned}[1] &= \{\ldots. - 11, -5, 1, 7, 13, 19, \ldots\} \\ &= \{1 + 6n \mid n \in \mathbb{Z}\}\end{aligned}$$

La relación $R_3 = \{(a,a),(a,b),(b,b),(b,a),(c.c)\}$ es de equivalencia en $A = \{a, b, c\}$; las clases de equivalencia determinadas por ellas son

$$[a]_{R_3} = \{a, b\} \quad \text{y} \quad [c]_{R_3} = \{c\}.$$

Para la relación de equipotencia definida en $\mathcal{P}(\{a,b,c\})$, se tienen las siguientes clases de equivalencia:

$$\begin{aligned}[\{a\}] &= \{\{a\},\{b\},\{c\}\}; \qquad [\emptyset] = \{\emptyset\} \\ [\{a,c\}] &= \{\{a,c\},\{a,b\},\{b,c\}\} \qquad \text{y} \\ [\{a,b,c\}] &= \{\{a,b,c\}\}.\end{aligned}$$

Nótese que $[\{a\}] = [\{b\}] = [\{c\}]$ y que $[\{a,c\}] = [\{a,b\}] = [\{b,c\}]$.

LEMA 1. *Sea R una relación de equivalencia sobre un conjunto A no vacío; si a, b son elementos cualesquiera de A, se tiene que:*

(i) $a \in [a]$.

(ii) *Las afirmaciones aRb, $a \in [b]$ y $[a] = [b]$ son equivalentes.*

Demostración.

(i) Por ser R reflexiva, aRa para todo a de A, luego $a \in \{a\}$. En consecuencia una clase de equivalencia nunca es vacía.

(ii) Siendo $[b] = \{x \in A | xRb\}$ y estando $a, b \in A$, es evidente que

$$aRb \leftrightarrow a \in [b]. \qquad (*)$$

Probemos entonces su equivalencia con $[a] = [b]$. Si $[a] = [b]$, como por (i) $a \in [a]$, necesariamente $a \in [b]$. Recíprocamente, supongamos $a \in [b]$ y demostremos que $[a] = [b]$:

1.	aRb	por $(*)$ de la hipótesis
2.	$x \in [a]$	hipótesis de trabajo
3.	xRa	por $(*)$ y 2.
4.	xRb	por transitividad de 1. y 3.
5.	$x \in [b]$	por $(*)$ y 4.
6.	$x \in [a] \rightarrow x \in [b]$	por 2. y 5.
7.	$x \in [b]$	hipótesis de trabajo
8.	xRb	por $(*)$ y 7.
9.	bRa	de 1. por simetría de R.
10.	xRa	de 8. y 9. por la transitividad de R
11.	$x \in [a]$	por $(*)$ y 10.
12.	$x \in [b] \rightarrow x \in [a]$	por 7. y 11.
13.	$x \in [a] \leftrightarrow x \in [b]$	por 6. y 12.
14.	$[a] = [b]$	por el axioma de extensión.

□

Dada una relación de equivalencia R en A, como una clase de equivalencia de un elemento de A es un subconjunto de A, podemos formar el conjunto de todas las clases de equivalencia con respecto a R de los elementos de A (notado A/R) con solo *separar* de $\mathcal{P}(A)$ aquellos elementos que sean clases de equivalencia según R, es decir,

$$A/R = \{Y \in \mathcal{P}(A) \mid (\exists x \in A)(Y = [x]_R)\}$$

Se le acostumbra llamar el *conjunto cociente* de A por R.

Con respecto a dos de los ejemplos anteriores, se tiene $\{a,b,c\}/R_3 = \{\{a,b\},\{c\}\}$ y

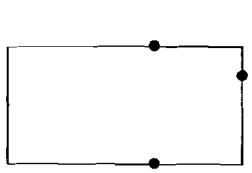
$$\begin{aligned}(\mathcal{P}(\{a,b,c\})/\equiv) = \{ &\{\emptyset\}, \{\{a\},\{b\},\{c\}\}, \{\{a,b\},\{a,c\},\{b,c\}\}, \\ &\{\{a,b,c\}\}\}\end{aligned}$$

TEOREMA 15. A/R es una colección de conjuntos no vacíos, disyuntos dos a dos y cuya unión es todo A.

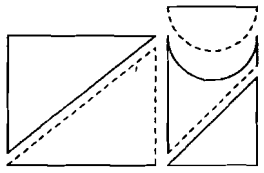
Demostración. por (i) del lema anterior sabemos que una clase de equivalencia nunca es vacía. También por (i) se obtiene que $\cup(A/R)$ es A, ya que todo elemento a de A pertenece al menos a su clase de equivalencia $[a]_R$ y además siempre $[a]_R \subseteq A$.

Para probar que las clases de equivalencia son disyuntas dos a dos, en vez de ver que $[a] \neq [b] \rightarrow [a] \cap [b] = \emptyset$, demostraremos su contrarrecíproca $([a] \cap [b] \neq \emptyset) \rightarrow ([a] = [b])$. En efecto, si $x \in [a] \cap [b], x \in [a]$ y $x \in [b]$ y por el lema anterior $[x] = [a]$ y $[x] = [b]$, de donde, por transitividad de la igualdad, $[a] = [b]$ quedando demostrado. □

Si uno toma una hoja A de papel y con unas tijeras la corta digamos en cinco pedazos, la colección de estos pedazos posee las mimas propiedades atribuidas a A/R en el teorema anterior:



A



Una partición de A

Los pedazos son no vacíos, disyuntos dos a dos y su unión es A; a una colección tal se le llama una *partición* de A.

DEFINICIÓN 22. *Una* partición *de un conjunto no vacío A es una colección de subconjuntos no vacíos de A, disyuntos dos a dos y cuya unión es A.*

Por ejemplo, entre las particiones de $\{a, b, c, d\}$ están las siguientes:

$$P_1 = \{\{a\}, \{b, c, d\}\},$$
$$P_2 = \{\{a, c\}, \{b\}, \{d\}\},$$
$$P_3 = \{\{a, d\}, \{b, c\}\}.$$

El teorema anterior nos dice que toda relación de equivalencia R en A determina una partición A/R del conjunto A; el recíproco también es cierto.

TEOREMA 16. Toda partición de un conjunto no vacío determina una relación de equivalencia sobre dicho conjunto.

Demostración. Sea P una partición de A, $A \neq \emptyset$; definamos en A la relación siguiente:

$$xRy \Leftrightarrow (\exists B \in P)(x \in B \wedge y \in B).$$

Es decir, dos elementos de A están relacionados si y sólo si pertenecen a un mismo pedazo de la partición.

Como $\bigcup_{B \in P} B = A$, todo elemento x de A pertenece a algún pedazo B de P, así que $x \in B \wedge x \in B$ o sea xRx.

Si xRy, existe B en P tal que $x \in B \wedge y \in B$; por la conmutatividad de la conjunción, $y \in B \wedge x \in B$, o sea yRx.

Supongamos $xRy \wedge yRz$; entonces existen B_1, B_2 que pertenecen a P tales que $(x \in B_1 \wedge y \in B_1) \wedge (y \in B_2 \wedge z \in B_2)$; como $y \in B_1 \cap B_2$, se deberá tener $B_1 = B_2$ ya que los conjuntos de P son disyuntos dos a dos, así que $x \in B_1 \wedge z \in B_1\ (= B_2)$, luego xRz. □

¿Cuáles son las clases de equivalencia determinadas por la relación anteriormente considerada? Precisamente los pedazos dados de la partición, ya que si a es un elemento de un pedazo B de P, la clase $[a]$ es el conjunto de los x de A tales que xRa, es decir que pertenecen al mismo B, luego $[a] = B$.

Pasemos ahora a un tema relacionado y de gran utilidad posterior. Supongamos que en un conjunto A se hallan definidas una operación binaria $* : A \times A \rightarrow A$ y una relación de equivalencia R. Queremos dar condiciones que nos permitan usar la operación anterior para definir de una manera natural una operación en *el conjunto cociente* A/R; deseamos mediante una operación entre elementos de A, inducir una operación entre clases de equivalencia.

DEFINICIÓN 23. *Se dice que una relación de equivalencia R sobre un conjunto A es compatible con una operación $*$ definida en A, si se tiene que para a, a', b, b' cualesquiera de A,*

$$aRa' \wedge bRb' \rightarrow (a * b)R(a' * b').$$

Nótese que la compatibilidad significa que si se cambian los operandos a y b por otros a' y b' respectivamente equivalentes, también los resultados de $a * b$ y $a' * b'$ son equivalentes. Si se tiene en cuenta el Lema 1 y se toman clases de equivalencia, la implicación anterior se transforma en

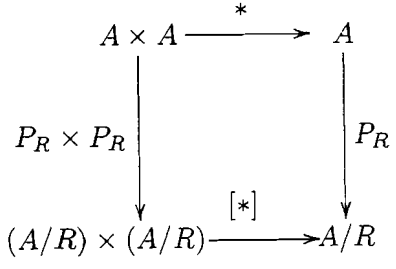
$$([a] = [a'] \wedge [b] = [b']) \rightarrow ([a * b] = [a' * b']).$$

Analizando esta expresión nos damos cuenta de que cuando hay compatibilidad, es posible definir una operación (notada $[*]$) entre clases de equivalencia en la forma siguiente:

$$[a][*][b] = [a * b]$$

La última implicación nos dice que $[*]$ está bien definida, que no hay ambigüedad y que realmente $[*]$ es una función de $A/R \times A/R$ en A/R; ($[*]$ no sería función si sucediese que $[a] = [a']$ y $[b] = [b']$ y que sin embargo $[a][*][b] \neq [a'][*][b']$).

Se dice que $[*]$ es la operación obtenida por *paso al cociente* de $*$. Si notamos por p_R a la función de A en A/R que a un elemento de A le hace corresponder su clase de equivalencia según R (se dice que p_R es la *proyección canónica* de A sobre A/R), la definición de la operación $[*]$ equivale a la conmutatividad del diagrama (a).



(a)

[+]	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

(b)

Ejercicio para el lector: verificarlo.

Apliquemos lo anterior a un caso particular; consideremos el conjunto $\mathbb{Z}$ de los entero con la adición; sabemos que la congruencia módulo tres es una relación de equivalencia en $\mathbb{Z}$; veamos que es compatible con la adición de enteros; supongamos $a \equiv a'(3) \wedge b \equiv b'(3)$; existen enteros r, s tales que $(a - a' = 3r) \wedge (b - b' = 3s)$; sumando miembro a miembro estas igualdades, $(a - a') + (b - b') = 3r + 3s$ o sea

$$(a + b) - (a' + b') = 3(r + s) \qquad \text{es decir}$$
$$a + b \equiv a' + b'(3)$$

quedando comprobada la compatibilidad; podemos entonces pasar al cociente la adición

$$[m][+][n] = [m + n].$$

Esta es una "adición" entre clases de equivalencia módulo tres, o sea en el conjunto $\mathbb{Z}/(3)$, notación que se usa para la colección de estas clases de equivalencia (en vez de $\mathbb{Z}/\equiv(3)$).

Por ejemplo $[2]_3 + [1]_3 = [2 + 1]_3 = [0]_3$.

Podemos expresar mediante una tabla dicha adición (fig. (b) anterior).

El resultado de operar un elemento x con otro y se halla en el cruce de la fila donde se encuentra x y de la columna donde está y.

Ejercicios

1. (a) Sea $f : A \to B$ cualquier función entre conjuntos no vacíos; pruebe que la relación R definida por $xRy \Leftrightarrow f(x) = f(y)$ es de equivalencia en A.
   (b) Si $f : \mathbb{R} \to \mathbb{R}$ está dada por $f(x) = x^2 - x + 2$, halle, con respecto a la relación de equivalencia definida en a), las clases de equivalencia de los reales 0, 2 y a.
   (c) Si S es una relación de equivalencia en A y $p_S : A \to A/S$ es la proyección canónica asociada, pruebe que S coincide con la relación R definida en (a) cuando $f = p_S$.

2. Pruebe que en $\mathbb{R}$ la relación

   $$xRy \Leftrightarrow Sen(x - y) = 0$$

   es de equivalencia. Halle para esta relación las clases de equivalencias de los reales, $0, \pi/2, \pi/4$ y a.

3. Sea $A = \{a, b, c\}$; halle todas las particiones del conjunto A; encuentre, dándolas como conjuntos de parejas ordenadas, las relaciones de equivalencia correspondientes a las particiones halladas.

4. (a) Halle el número de particiones que existen para un conjunto con 4 elementos.
   (b) Id. para un conjunto con 5 elementos.

5. Demuestre que en $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ la relación siguiente es de equivalencia:

   $$(m, n)R(p, q) \text{ si y sólo si } mq = np.$$

   Halle $[(-2, 6)]_R$ y $[(0, 1)]_R$.

6. (a) Pruebe que en $\mathbb{R}$ la relación

$$xSy \text{ si y sólo si } x^2 - y^2 = 3x - 3y$$

es de equivalencia. Halle $[0]_S, [2]_S$ y $[a]_S$

(b) Id. para xTy si y sólo si $x^3 + 2y = y^3 + 2x$. Halle $[3]_T$ y $[5]_T$

7. Si R_1, R_2 son relaciones de equivalencia en A,

(a) Pruebe que $R_1 \cap R_2$ es también de equivalencia.

(b) Dé un contraejemplo para hacer ver que en general $R_1 \cup R_2$ *no* es una relación de equivalencia.

8. Halle el error de la siguiente "demostración" de que las propiedades simétrica y transitiva implican la reflexiva.

(0) Supongamos aRb.

(1) Se deduce entonces bRa por simetría.

(2) De (0) y (1) por transitividad se deduce aRa.

(3) Luego R es reflexiva.

9. Definimos en $\mathbb{R}^2$ la relación

$$(x, y)R(u, v) \Leftrightarrow (\exists m, n \in \mathbb{Z})(x = u + m \wedge y = v + n).$$

(a) Demuestre que es de equivalencia.

(b) Localice en un gráfico $[(0, 0)]_R$ y $[(1/2, 10/3)]_R$.

(c) Pruebe que toda pareja ordenada (x, y) de $\mathbb{R}^2$ es equivalente según R con un único punto de $[0, 1) \times [0, 1)$.

10. Sea $*$ una operación conmutativa definida en un conjunto A; pruebe que una relación de equivalencia R en A es compatible con $*$ si y sólo si

$$(\forall x, y, z \in A)(xRy \rightarrow (x * z)R(y * z)).$$

11. Consideremos en $\mathbb{Z}$ la relación de congruencia módulo m.

(a) Demuestre que nunca dos elementos del conjunto

$\{0, 1, 2, ..., m - 1\}$ pueden ser congruentes entre sí módulo m.

(b) Pruebe que todo entero es congruente módulo m con un único elemento del conjunto $\{0, 1, 2, ..., m - 1\}$.

(c) Deduzca de (a) y (b) que

$$\mathbb{Z}/(m) = \{[0], [1], [2], ..., [m - 1]\}.$$

12. Pruebe que en $\mathbb{Z}$ la congruencia módulo 3 también es compatible con la multipliación de enteros. En consecuencia, defina "multiplicación" en $\mathbb{Z}/(3)$ y construya la tabla para dicha operación.

13. (a) Pruebe que en $\mathbb{Z}$ la relación de congruencia módulo m es compatible tanto con la adición como con la multiplicación usuales; pase estas operaciones al cociente $\mathbb{Z}/(m)$ y halle tanto $[2]_m[+][m - 1]_m$ como $[m - 3] \cdot [0]$.

(b) Construya la tabla para la adición y la multiplicación así obtenidas en $\mathbb{Z}/(6)$.

*14. Demuestre que $\mathbb{Z}/(5)$ con $[+]$ y $[\cdot]$ es un cuerpo conmutativo.

15. Sea R una relación de equivalencia en un conjunto A y sea $M \subseteq A$. Diremos que $\mathbb{Z}$ es una *parte saturada* de A para R si

$$(\forall a, x \in A)(a \in M \wedge xRa \rightarrow x \in M).$$

Demuestre que M es saturado para R si y sólo si M es unión de clases de equivalencia según R.

3.7 RELACIONES DE ORDEN

DEFINICIÓN 24. *Una relación R en un conjunto A se llama una* **relación de orden en** *A si R es reflexiva, antisimétrica y transitiva en A. Se acostumbra decir que A es un conjunto ordenado por R.*

Por ejemplo, de las relaciones dadas en la sección 5, son de orden la R_2 de (1), la igualdad entre elementos de A, la contenencia entre subconjuntos de un conjunto dado y las descritas en (4) y (8).

Para las relaciones de orden usaremos, en vez de R, como notación $\preceq$ o algún símbolo semejante y leeremos "$x \preceq y$" como "x precede a y" ó "x es menor que o igual a y".

Sea $\preceq$ una relación de orden en A; un subconjunto B de A se llama *totalmente ordenado* por $\preceq$ o una *$\preceq$-cadena* en A, si

$$(\forall x, y \in B)[(x \preceq y) \vee (y \preceq x)]$$

es decir, si todos sus elementos son comparables mediante $\preceq$.

Si en un subconjunto P de A existen elementos a y b tales que $\neg(a \preceq b) \wedge \neg(b \preceq a)$, se dice que P es *parcialmente ordenado* por $\preceq$. Cuando el conjunto completo A es totalmente ordenado por $\preceq$, se dice que $\preceq$ es una *relación de orden total o lineal en A*; en caso contrario se dice que es una relación de orden tan sólo parcial en A.

Si consideramos al conjunto $A = \{1, 2, 3, 4, 5, ..., 14, 15, 15\}$ ordenado mediante la relación "es divisor de" (o sea $x \preceq y$ si y sólo si x es divisor de y), el subconjunto {1,3,6,12} es totalmente ordenado por dicha relación mientras que A o {1,2,3,4} no lo son, así que esta relación solo ordena parcialmente a A.

Las relaciones de orden usual en $\mathbb{N}$, en $\mathbb{Z}$ o en $\mathbb{R}$ son de orden total.

Aun cuando en lo referente al orden no todos los autores usan los mismos términos técnicos con los mismos significados, elegiremos los de empleo más frecuente o los que más concuerdan con el uso corriente, de tal manera que por lo menos en cuanto a ordenes totales se refiere, las definiciones son bastante intuitivas y al lector solo le restará manejarlas con un poco de cuidado en los casos en que se apliquen a órdenes parciales.

Si $\preceq$ es una relación de orden en A, a la relación $\prec$ definida mediante $x \prec y \leftrightarrow (x \preceq y \wedge x \neq y)$ se le llama el *orden estricto o riguroso* correspondiente a $\preceq$ (se obtiene suprimiendo de $\preceq$ las parejas ordenadas que posean sus dos componentes iguales); "$x \prec y$ se puede leer "x precede rigurosa o estrictamente a y". Esta relación posee las propiedades

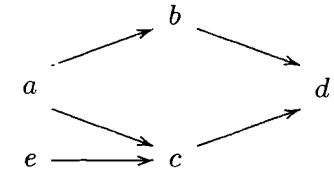
$$(\forall x, y \in A)(\neg(x \prec y \wedge y \prec x)) \quad (ASIMETRIA)$$
$$(\forall x, y, z \in A)((x \prec y \wedge y \prec z) \rightarrow x \prec z).$$

La primera se llama la *asimetría* de la relación y es equivalente en el lenguaje de la teoría de conjuntos a: $(\forall x, y \in A)(x \prec y \rightarrow \neg(y \prec x))$. Se deduce de la antisimetría de $\preceq$, ya que si $x \neq y$, entonces $\neg(x \preceq y \wedge y \preceq x)$. En particular se obtiene $(\forall x \in A)(\neg(x \prec x))$ (*irreflexividad*).

La segunda es simplemente la transitividad de la relación.

Recíprocamente, si una relación $\prec$ en A goza de las dos propiedades anteriores, ella determina una única relación de orden en A con simplemente adjuntarle todas las parejas (a, a) con a en A, es decir definiéndola como $x \preceq y \leftrightarrow [x \prec y \vee x = y]$.

Por ésto muchas veces diremos "sea el conjunto $\{a, b, c, d, e\}$ ordenado según el diagrama que sigue"



Se sobrentiende que sólo se ha representado el orden estricto y que un elemento precede al otro si se puede ir del primero al segundo siguiendo el camino indicado por las flechas. En términos de parejas ordenadas, la relación de orden estricto descrita en el diagrama no es otra que

$$\prec = \{(a, b), (a, d), (a, c), (b, d), (c, d), (e, c), (e, d)\}$$

y en consecuencia

$$\preceq = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, d), (a, d), (a, c), (c, d), (e, c), (e, d)\}.$$

DEFINICIÓN 25. *Sea $\preceq$ una relación de orden en A y sea B un subconjunto no vacío de A. Un elemento a de A se llama* **el primero, el menor o el mínimo de** *B si* (i) $a \in B$ y (ii)$(\forall x \in B)(a \preceq x)$.

Es evidente que cuando tal a existe es único, ya que si a' también fuese un primero de B, por (i) a' estaría en B y por (ii), $a \preceq a'$ (a es el menor de B) y $a' \preceq a$ (a' es el menor de B), de donde $a = a'$ por la antisimetría.

DEFINICIÓN 26. *Sea A ordenado por $\preceq$ y sea B un subconjunto no vacío de A. Se dice que un elemento u de A es* `el último, el mayor o el máximo de` *B si* (i) $u \in B$ *y* (ii)$(\forall x \in B)(x \preceq u)$.

De manera similar, el máximo cuando existe es único.

Por ejemplo, si A es el conjunto de las letras del alfabeto ordenado en la forma usual, a es el primero y z el último de A.

Si $A = \mathbb{N}$ con el orden usual, cero es el primero de $\mathbb{N}$ y 2 sería el menor del subconjunto B de todos los números primos; en este caso ni A ni B poseen último elemento.

Cuando $A = \mathcal{P}(\{a, b, c\})$ ordenado por inclusión , $\emptyset$ es el primero y $\{a, b, c\}$ es el último de A, pero el conjunto

$$B = \{\{a\}, \{b\}, \{c\}, \{a, b\}\}$$

no tiene primero ni último.

Si $A = \mathbb{R}$ ordenado en la forma usual y $B = \{x \in \mathbb{R} \mid 0 < x < 2\}$, ni A ni B poseen primero ni último elementos.

Esta misma situación se presenta con frecuencia en conjuntos arbitrarios totalmente ordenados; se hace necesario introducir conceptos con requerimientos más débiles, que desempeñen papeles similares a los de primero y último.

DEFINICIÓN 27. *Sean $\preceq$ una relación de orden en A y B un subconjunto de A.* `Una cota inferior de` *B es cualquier elemento m de A tal que $(\forall x \in B)(m \preceq x)$. Una* `cota superior de` *$B$ es cualquier elemento s de A tal que $(\forall x \in B)(x \preceq s)$.*

DEFINICIÓN 28. *Sean A un conjunto ordenado por $\preceq$ y B un subconjunto de A; llamaremos ínfimo de B (abreviado $Ínf\ B$) a la máxima de las cotas inferiores de B, cuando exista. Análogamente, llamaremos supremo de B (abreviado $Sup\ B$) a la mínima de las cotas superiores de B, cuando exista.*

Si adoptamos las notaciones

$B_* =$ Conjunto de las cotas inferiores de B

$B^* =$ Conjunto de las cotas superiores de B

entonces, cuando $Ínf\ B$ y $Sup\ B$ existen, se tiene que

$Ínf\ B =$ máximo de $B_* =$ último de B_*

$Sup\ B =$ mínimo de $B^* =$ primero de B^*.

Siendo el mínimo y el máximo únicos cuando existen, se deduce que $Ínf\ B$ y $Sup\ B$ son únicos cuando existen.

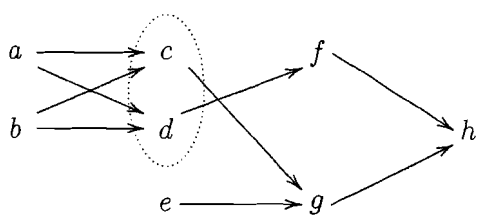
Por ejemplo, si $A = \mathbb{R}$ con el orden usual y $B = (1, 4]$, se tiene $B_* = (-\infty, 1]$, $Ínf\ B = 1$, $B^* = [4, +\infty)$ y $Sup\ B = 4$. Similarmente, si C es el conjunto de los racionales mayores que cero, entonces $C_* = (-\infty, 0]$, $Ínf\ C = 0$, $C^* = \emptyset$ y $Sup\ C$ no existe.

Obsérvese que algunas veces $(Ínf\ B) \notin B$ y otras sí; es realmente trivial ver que $(Ínf\ B) \in B$ si y sólo si $Ínf\ B =$ primero de B y que $(Sup\ B) \in B$ si y sólo si $Sup\ B =$ máximo de B, de modo que $Ínf$ y Sup se constituyen realmente en generalizaciones de mínimo y máximo, respectivamente. Consideremos $A = \mathbb{N} - \{0\}$ ordenado mediante "es divisor de" y sea $B = \{12, 30, 20\}$; se tiene entonces $B_* = \{1, 2\} =$ Conjunto de divisores comunes de 12, 30 y 20.

$$B^* = \{60, 120, 180, 240, ...\} = \text{Conjunto de múltiplos comunes de 12, 30 y 20.}$$

$$Ínf\ B = \text{Máximo Com. Div. de 12, 30 y 20} = 2$$
$$Sup\ B = \text{Mín. Com. Mult. de 12, 30 y 20} = 60\ .$$

Ordenemos el conjunto $A = \{a, b, c, d, e, f, g, h\}$ de acuerdo con el diagrama adjunto. Si $B = \{c, d\}$ entonces $B_* = \{a, b\}$ pero $Inf\ B$ no existe ya que ni a precede a b ni b a a; $B^* = \{h\}$ ya que h es el único elemento precedido simultáneamente por c y d; evidentemente $Sup\ B =$ mín. de $B^* = h$. Obsérvese que B no posee primero ni último elementos. El conjunto A tiene último elemento y es h, pero no posee mínimo; sin embargo existen en él elementos que no son precedidos rigurosamente por otros, como a, b y e; a éstos se les acostumbra llamar elementos minimales de A.



DEFINICIÓN 29. *Sea A un conjunto ordenado por $\preceq$ y B un subconjunto no vacío de A. Se dice que l es un* `elemento minimal de` *B si*

i) $l \in B$ y

ii) $\neg(\exists x \in B)(x \prec l)$.

La condición ii) también se puede dar bajo la forma $(\forall x \in B)(\neg(x \preceq l \wedge x \neq l))$ o sea $(\forall x \in B)[\neg(x \preceq l) \vee (x = l)]$, equivalente a $(\forall x \in B)(x \preceq l \rightarrow x = l)$.

Análogamente, s es un *elemento maximal* de B si $s \in B$ y $\neg(\exists x \in B)(s \prec x)$ o $(\forall x \in B)(s \preceq x \rightarrow s = x)$ es decir que s es maximal de B si está en B y no existen elementos de B que sucedan rigurosamente a s.

La idea intuitiva de que máximo y mínimo, maximal y minimal, *Sup* e *Ínf* son especies de duales los unos de los otros, puede concretarse en la forma siguiente:

DEFINICIÓN 30. *Llamaremos relación de orden opuesto al orden $\preceq$ en A, a la relación notada $\succeq$ dada por*

$$\succeq = \{(y,x) | (x,y) \in \preceq\} = \preceq^{-1}$$

es decir que $y \succeq x \leftrightarrow x \preceq y$.

Es entonces evidente que el mínimo para el orden "$\preceq$" es precisamente el máximo para "$\succeq$" y lo mismo sucede con los otros conceptos.

DEFINICIÓN 31. *Sea $\preceq$ una relación de orden en A; se dice que A es* `bien ordenado` *por $\preceq$ (o que $\preceq$ es un* `buen orden` *para A) si todo subconjunto no vacío de A tiene primer elemento con respecto al orden $\preceq$.*

El prototipo de conjunto bien ordenado es $\mathbb{N}$ con su orden usual.

TEOREMA 17. *Todo conjunto bien ordenado es totalmente ordenado, o con más precisión: toda relación de orden que es un buen orden, es un orden total.*

Demostración. Sea $\preceq$ un buen orden para A y sean x, y elementos cualesquiera de A. Como el subconjunto $\{x,y\}$ de A es no vacío, deberá tener primer elemento; si éste es x, entonces $x \preceq y$ y si es y, $y \preceq x$ luego "$\preceq$" es un orden total puesto que mediante él dos elementos cualesquiera son comparables. □

El recíproco no es cierto; por ejemplo $\mathbb{Z}$ con su orden usual es totalmente ordenado y no es bien ordenado, ya que si lo fuese, el mismo $\mathbb{Z}$ debería tener primer elemento, lo cual no es así.

Para no cansar al lector con más definiciones, incluiremos dentro de los ejercicios otros conceptos adicionales que servirán además para aclarar ideas y eliminar algunas de las dudas surgidas.

Ejercicios

1. Diga cuáles de las relaciones siguientes son de orden y de estas últimas, cuáles de orden total y cuáles de buen orden. Dé las razones de sus respuestas.

   (a) $(x,y)R(u,v) \leftrightarrow (x^2 + y^2 \leq u^2 + v^2)$, relación en $\mathbb{R}^2$.

   (b) $\{(1,1),(1,a),(a,c),(1,b),(b,b),(a,a),(1,c),(c,c)\} = R$ definida en el conjunto $\{1,a,b,c\} = \mathcal{D}(R)$.

   (c) $xSy \leftrightarrow (x^2 - y \leq y^2 - x)$, relación en $\mathbb{R}$.

   (d) Si A = conjunto de todos los triángulos de un plano fijo provisto de un sistema coordenado, definimos $X \preceq Y \leftrightarrow (a(X) \leq a(Y))$ donde $a(X)$ denota el área de X y $\leq$ es el orden usual de $\mathbb{R}$.

   (e) $(\frac{m}{n} \preceq \frac{p}{q}) \leftrightarrow (mq \leq np)$ en $\mathbb{Q}$, siendo $\leq$ el orden usual de $\mathbb{Z}$.

2. Halle todas las relaciones de orden (dándolas mediante diagramas y mediante conjuntos de parejas ordenadas) que existen en el conjunto $\{*, \square, \triangle\}$

3. Si $A = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y \geq 0\}$, pruebe que la siguiente es una relación de orden en A:
   $(x,y) \preceq (u,v) \leftrightarrow (x < u \vee (x = u \wedge (x^2 + y^2 \leq u^2 + v^2)))$.
   ¿Es un orden total en A?

   Si $B = \{(x,y) \in A \mid 1 < x^2 + y^2 \leq 4\}$ y $C = \{(x,y) \in A : |y| \leq 2\}$, halle B_*, B^*, C_*, C^*, $Sup\ B$, $Ínf\ B$, $Sup\ C$, $Ínf\ C$ si existen.

4. (a) Pruebe que dado $a \in \mathbb{N} - \{0\}$, existen $n, m \in \mathbb{N}$ únicos tales que $a = 2^n(2m+1)$.

(b) Demuestre que la siguiente es una relación de orden total en $A = \mathbb{N} - \{0\}$: Si $a, b \in \mathbb{N} - \{0\}$, expresémoslos en la forma $a = 2^n(2m+1)$ y $b = 2^r(2s+1)$.
Entonces definimos $a \preceq b \leftrightarrow (n < r \vee (n = r \wedge m \leq s))$.
¿Es un buen orden en A? ¿Tiene A primer elemento?
Si $B = \{12, 14, 15\}$, halle para el orden definido en a) B_*, B^* y $Sup\ B$, $Inf\ B$, si existen.

5. Pruebe que $(x, y) \preceq (a, b) \Leftrightarrow (x \leq a \wedge y \leq b)$ es una relación de orden en $\mathbb{N} \times \mathbb{N}$, donde $\leq$ es el orden usual de $\mathbb{N}$.

   ¿Es un orden total? ¿Es un buen orden? ¿Tienen $\mathbb{N} \times \mathbb{N}$ primer elemento? ¿Tiene elementos minimales?

   Si $A = \{(1,1), (1,2), (3,4), (2,2), (5,9), (5,4)\}$, halle A_*, A^* y $Sup\ A$ e $Inf\ A$ si existen.

   Si $B = \{(1,2), (2,3), (5,6)\}$, halle B_*, B^* y $Sup\ B$ e $Inf\ B$ si existen.

*6. Dé un ejemplo de un conjunto parcialmente ordenado que posea un único elemento maximal y que sin embargo éste no sea máximo.

*7. Pruebe que todo conjunto finito no vacío totalmente ordenado es bien ordenado.

8. Un conjunto ordenado se llama *dirigido o filtrante* a derecha si todos sus subconjuntos con dos elementos son acotados superiormente; se llama dirigido o filtrante a izquierda si todos sus subconjuntos con dos elementos son acotados inferiormente.

   Dé un ejemplo de un conjunto filtrante a derecha y no a izquierda y otro que sea filtrante a izquierda y no a derecha.

   Dé dos ejemplos de conjuntos filtrantes (es decir a derecha y a izquierda simultáneamente) y que no sean totalmente ordenados.

9. Pruebe que si "$\preceq$" es un orden filtrante en A y A posee un único elemento maximal, entonces éste es el último elemento de A.

10. Un conjunto ordenado por "$\preceq$" se llama *un conjunto reticular o un retículo* si todos sus subconjuntos con dos elementos poseen Inf y Sup.

    Dé dos ejemplos de conjuntos reticulares que no sean totalmente ordenados.

Dé un ejemplo de un conjunto ordenado que sea dirigido y no sea reticular.

Un retículo se llama *completo* si todo subconjunto no vacío de él tiene Inf y Sup. Dé un ejemplo de un retículo completo que no sea totalmente ordenado.

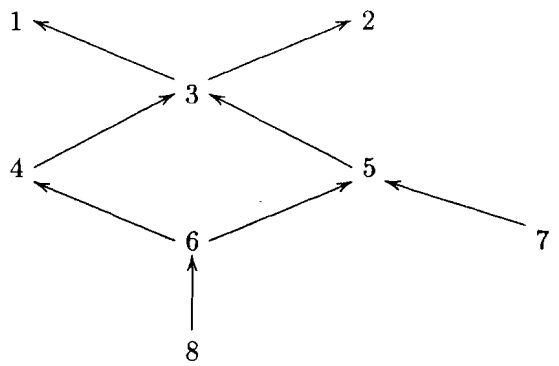
11. Haga un diagrama para representar $A = \mathcal{P}(\{a, b, c\})$ ordenado por inclusión.

    Si $B = \{\{a, b\}, \{a, d\}\}$, halle B_*, B^* y $Sup\ B$ e $Inf\ B$ (si existen). ¿Es filtrante? ¿Es reticulado?

12. Sea A un conjunto ordenado por $\preceq$ y sea B un subconjunto no vacío de A; pruebe que la relación $\preceq \cap (B \times B)$ es un orden de B. Se llama el *orden inducido* por $\preceq$ en B.

    Si consideramos al conjunto $B = \mathbb{N} - \{0, 1\}$ con el orden inducido por "es un divisor de" dado en $A = \mathbb{N} - \{0\}$, ¿posee elementos minimales? ¿Cuáles? ¿Es B reticulado?

13. Sea $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ ordenado según el diagrama adjunto



    ¿Tiene A primer elemento? ¿Tiene útimo elemento? ¿Tiene A elementos minimales o maximales? ¿Cuáles?

    Si $B = \{4, 5, 6\}$, halle B_*, B^* y $Sup\ B$ e $Inf\ B$ si existen.

14. Dé razones para respaldar la afirmación "El orden de

$$\mathbb{Q}^+ = \{x \in \mathbb{Q} \mid x > 0\}$$

inducido por el orden usual de $\mathbb{R}$ no es un buen orden".

Demuestre que la siguiente relación es *un buen orden para* $\mathbb{Q}^+$: si $x \in \mathbb{Q}^+$, existen m, n naturales mayores que cero únicos tales que $x = \frac{m}{n}$ con $\frac{m}{n}$ irreductible, es decir con 1 como Max. Com. Div. de m y n.

Si $y = \frac{p}{q}$ está dado en la misma forma, definimos
$\frac{m}{n} \preceq \frac{p}{q} \leftrightarrow (n < q \vee (n = q \wedge m \leq p))$
donde $<$ y $\leq$ son las relaciones de orden usuales de $\mathbb{N}$.

¿Podría extenderse la idea anterior para definir una relación que sea un buen orden de todo $\mathbb{Q}$?

15. La relación de orden con la cual se hallan ordenadas en un diccionario las palabras de una lengua se llama el *orden lexicográfico*. Como las palabras son énuplas ordenadas de letras, podemos copiar en matemáticas la misma idea para ordenar productos cartesianos finitos de conjuntos ordenados: Si A_1, A_2, A_3 son conjunto ordenados (notamos $\leq$ al orden de cada uno de ellos), pruebe que la siguiente relación es de orden en $A_1 \times A_2 \times A_3$: $(x_1, x_2, x_3) \preceq (y_1, y_2, y_3)$ si y sólo si $(x_1 < y_1) \vee (x_1 = y_1 \wedge x_2 < y_2) \vee (x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 \leq y_3)$, o sea: de dos "palabras" de tres letras, está antes la que tenga menor la primera letra y si las primeras letras son iguales, está antes la que tenga menor la segunda, y si las dos primeras letras son iguales, usamos la tercera para decidir. El proceso se puede repetir finitas veces para ordenar el producto cartesiano de una colección finita de conjuntos ordenados.

Pruebe que si $A_1, A_2, A_3, ..., A_n$ son totalmente ordenados, también lo es $A_1 \times A_2 \times A_3 \times ... \times A_n$ con el orden lexicográfico. Demuestre que si $A_1, A_2, A_3, ..., A_n$ son conjuntos bien ordenados, también lo es $A_1 \times A_2 \times A_3 \times ... \times A_n$ con el orden lexicográfico.

16. Halle tres relaciones de orden total para el conjunto $\mathbb{C}$ de los complejos.

17. Decimos que una relación R es de orden (a secas) si R es un relación de orden en el campo de la relación

$$\tau(R) = \mathcal{D}(R) \cup \mathcal{R}(R).$$

(a) Pruebe que si $\mathcal{O}$ es una colección de relaciones de orden tales que $(\forall R \in \mathcal{O})(\forall S \in \mathcal{O})(R \subseteq S \vee S \subseteq R)$, entonces $\bigcup_{R \in \mathcal{O}} R$ es también una relación de orden.

(b) Si toda relación R de $\mathcal{O}$ ordena totalmente a su campo $\tau(R)$, entonces $\bigcup_{R \in \mathcal{O}} R$ ordena totalmente a su campo

$$\tau(\bigcup_{R \in \mathcal{O}} R) = \bigcup_{R \in \mathcal{O}} \tau(R).$$

*18. Sea $\mathfrak{F}$ un conjunto de funciones ordenado por inclusión; pruebe que si $\mathfrak{C}$ es una $\subseteq$-cadena en $\mathfrak{F}$, entonces $\cup\mathfrak{C}$ también es una función; si todas las funciones de $\mathfrak{C}$ son inyectivas, demuestre que $\cup\mathfrak{C}$ también lo es.

19. A un conjunto ordenado $(A, \preceq)$ se le llama *denso* para el orden dado (u *orden denso, o que* $\preceq$ *es un orden denso para* A), si entre todo par de elementos distintos de A siempre existe otro elemento de A, es decir si

$$(\forall x)(\forall y)(x \prec y \longrightarrow (\exists z)(x \prec z \wedge z \prec y)$$

(a) Pruebe que $\mathbb{Q}$ con el orden usual es denso.

(b) Demuestre que $\mathbb{R}$ con el orden usual es denso.

(c) ¿Podrá ser denso un conjunto ordenado finito?

(d) ¿Podrá ser denso un conjunto bien ordenado? ¿Y uno parcialmente ordenado?

Dé las razones de sus respuestas.

**

Capítulo 4

LOS NÚMEROS NATURALES

Existe desde hace mucho tiempo el convencimiento bien fundamentado por cierto, de que prácticamente toda la matemática descansa en la teoría de los números naturales [1]; en la escuela y en la secundaria, según los profesores y los programas oficiales que nos hayan correspondido, hemos recorrido el camino de los números naturales a los enteros, de éstos a los racionales, de estos últimos a los reales para llegar finalmente a los complejos. Esta misma senda se constituirá en nuestro programa a realizar en los capítulos IV y V de la presente introducción a la teoría de conjuntos.

Considerándose entonces los números naturales como la estructura básica de la Matemática, no es de extrañar que ellos se hayan estudiado casi exhaustivamente. Varios sistemas de postulados han sido propuestos para tratarlos axiomáticamente, para encuadrarlos dentro del modelo hipotético-deductivo hoy en boga en la Matemática; debido a su "naturalidad" y a los pocos conceptos primitivos que se usan, el conjunto de axiomas propuesto por el matemático italiano Giuseppe Peano ha tenido aceptación universal; los únicos términos técnicos que intervienen son los de número natural, primer número natural (cero para nosotros y uno para otros, según los gustos) y "el siguiente de" o "el sucesor de". Sus axiomas se han llegado a considerar como la base de todos los conocimientos matemáticos y al igual que los de Euclides, son cinco:

N1 - 0 es un número natural.

N2 - El siguiente de todo número natural también es un número natural.

[1] Quizás por esto llegó el matemático alemán Leopoldo kronecker a decir "El buen Dios nos dio los números naturales; el resto ha sido obra nuestra".

N3 - Si S es una colección de números naturales que cumple

i) 0 está en S

ii) Cada vez que un natural está en S, también el siguiente de él está en S

entonces S es el conjunto de todos los números naturales.

N4 - 0 nunca es el sucesor de un natural.

N5 - Si los siguientes de dos números naturales son iguales, entonces los números son iguales.

Es fascinante ver cómo se comienza a desarrollar por ejemplo la aritmética y el análisis a partir de estos sencillos axiomas; lo haremos parcialmente un poco más adelante.

4.1 CONSTRUCCIÓN DE LOS NATURALES

Si no nos conformamos con considerar "número natural" como un concepto primitivo y queremos ir más hacia el fondo del asunto, debemos preguntarnos: ¿Cómo podemos definir los números naturales? o más concretamente, por ejemplo, ¿Qué es el número tres?

Nuestra intuición nos dice que conjuntos como $\{a,b,c\}$, $\{\triangle,*,\square\}$, $\{Pedro, Luis, Juan\}$ poseen *tres* elementos; si nos preguntamos qué hay en común en ellos, nos responderemos que *son equipotentes*; podríamos entonces proponer la siguiente definición del número tres:

"*tres* es la propiedad común a *todos* los conjuntos equipotentes con $\{a,b,c\}$ ".

Aun cuando es una primera aproximación bastante buena, aceptable y adecuada para ciertos niveles (los de la escuela primaria, y aun secundaria, por ejemplo), dentro de nuestro estudio a "alto nivel" falla en puntos esenciales: 1) ¿Qué es una propiedad? 2) ¿Cómo hacemos para saber si es común a todos los conjuntos equipotentes con $\{a,b,c\}$? y más secundariamente, 3) ¿Qué sucede si en vez de $\{a,b,c\}$ escribimos $\{\triangle,*,\square\}$?

Para no usar el concepto "propiedad", no definido en nuestro estudio podemos emplear una idea que se utiliza con éxito algunas veces: identifica la propiedad en cuestión con el conjunto de todos los objetos que la poseen obtenemos entonces como "definición perfeccionada":

"Tres es la colección de todos los conjuntos equipotentes con $\{a,b,c\}$ " o sea

$$3 = \{A \mid A \approx \{a,b,c\}\}$$

El que en vez de $\{a,b,c\}$ se escriba

$$3 = \{A \mid A \approx \{\triangle,*,\square\}\}$$

no produce cambio alguno debido a que la equipotencia es reflexiva, simétrica y transitiva.

A primera vista esta definición parece bastante correcta; es en esencia la misma que dio el lógico y matemático alemán Gottlob Frege; él definió "el número de elementos de un conjunto" o sea "el cardinal de un conjunto" en la forma

$$\#(M) = \{A \mid A \approx M\}$$

En vez de $\#(M)$ para representar al cardinal de M, Cantor usó la notación $\bar{M}$ para indicar que se necesita efectuar dos abstracciones para llegar al concepto de cardinal: se debe prescindir tanto de la naturaleza de los elementos de M como del orden en el cual se hallan dispuestos. De acuerdo con ella,

$$3 = \#(\{a,b,c\}) = \{A \mid A \approx \{a,b,c\}\};$$

es precisamente nuestra definición anterior.

Surgen sin embargo objeciones realmente serias:

a) Nunca terminaríamos de definir todos los números naturales porque deberíamos definirlos uno por uno, dando una definición para cada número.

b) Dentro de nuestro tratamiento de la teoría de conjuntos, no nos está permitido formar los "conjuntos" usados para definir en la forma propuesta los naturales; por ejemplo $\{A \mid A \approx \{a,b,c\}\}$ no existe lícitamente ya que no se está cumpliendo con las limitaciones impuestas a las definiciones por comprensión; el axioma-esquema de separación nos exige aplicar la condición "$A \approx \{a,b,c\}$" a los elementos de un cierto conjunto S para obtener el conjunto $\{A \in S \mid A \approx \{a,b,c\}\}$. Pero este último depende de S y a lo más definirá el concepto "tres" para los elementos de S, de modo que si por ejemplo $\{\triangle,*,\square\}$ no está en S, no podemos en rigor afirmar que tenga tres elementos; en

consecuencia se quedarían sin cardinal aquellos conjuntos que no sean elementos de S. Recordemos además que estamos tratando de caracterizar "la propiedad de tener tres elementos" como aquella propiedad común a todos los conjuntos de la colección $\{A \in S \mid A \approx \{a,b,c\}\}$, pero nunca podemos estar seguros de que ésta sea la única propiedad común a tales conjuntos; podrían existir otras, todo depende de S.

c) Por otra parte si quisiésemos definir en la forma anterior todos los naturales a partir del mismo S, para cada natural deberían existir en S conjuntos con tantos elementos como dicho natural (o en caso contrario la definición daría como resultado el conjunto vacío); dicho conjunto S tendría que ser entonces *infinito*, debiéndose, postular antes la existencia de conjuntos infinitos.

Concluimos que si se quiere conservar la definición original de cardinal dada por Frege, es necesario considerar una teoría donde se permita la existencia de objetos tales como $\{A \mid A \approx \{a,b,c\}\}$, los cuales realmente no son conjuntos; dicha teoría no es otra que la "Teoría de Clases" propuesta por Von Neumann. Sin embargo la definición original debe modificarse ya que $3 = \{A \mid A \approx \{a,b,c\}\}$ es una "clase propia", o sea que no es un conjunto y no puede ser elemento de otra clase, de tal manera que no podría existir una clase cuyos elementos fuesen los números naturales.

Dentro de la teoría de conjuntos de Zermelo-Fraenkel que estamos desarrollando nos quedan dos alternativa; la primera consiste en no definir los cardinales, en tomar este concepto como primitivo y añadir como axioma $\#(A) = \#(B)$ si y sólo si $A \approx B$ (ver por ejemplo Suppes, P.,[9]). En esta forma se puede realizar el estudio sin mayores problemas definiéndose luego los naturales como los cardinales de los conjuntos finitos.

La segunda alternativa, la cual satisface nuestra inquietud de definir en verdad los naturales en términos de conjuntos y de paso asignar a la teoría de conjuntos el papel de "base de todo conocimiento matemático", consiste en definir los números naturales como los números ordinales finitos, siendo un ordinal un cierto conjunto bien ordenado. De esta manera no sólo produciremos *todos los naturales a la vez*, sino que los obtendremos dotados de una superestructura de la cual nos valdremos un buen trecho: todo natural será un conjunto bien ordenado, con la pertenencia como relación de orden estricto. Describiremos primero el procedimiento de manera informal y luego lo haremos rigurosamente, siguiendo las ideas sugeridas por Paul Halmos en su magnífico libro "Teoría intuitiva de los conjuntos" (ver [5]).

Analicemos cómo se definió "metro"; tan sólo como la "distancia que hay entre dos marcas hechas sobre una barra de platino-iridio conservada

en la oficina de pesas y medidas de Sevres"; no se ha definido como una "propiedad común a una clase de objetos equilongitudinales" ni nada por el estilo; simplemente se ha elegido un objeto atendiendo a razones de tipo práctico y a su longitud se le ha llamado metro; algo semejante puede hacerse para definir el tamaño de un conjunto, su número de elementos y en particular los números naturales. Por ejemplo, elijamos un conjunto con tres elementos y a él llamémosle "número tres"; ¿qué criterios podemos tener en cuenta para efectuar tal elección? Tal vez de sencillez, de familiaridad o de economía en el simbolismo. El conjunto que más conocemos es el vacío y siendo el único con cero elementos, es decir, siendo el único candidato, necesariamente debemos elegirlo como cero: $0 = \emptyset$. Como uno se podrá tomar $\{\emptyset\}$, conjunto del cual estamos completamente seguros que posee un único elemento; como número dos se podrá elegir el conjunto que contiene como elementos a los dos anteriores: $\{\emptyset, \{\emptyset\}\}$; también aquí estamos absolutamente seguros de que el conjunto posee dos elementos puesto que $\emptyset \neq \{\emptyset\}$. Análogamente definiríamos $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, $4 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$, etc.

Equivalentemente y con mayor economía de escritura, se tendría: $0 = \emptyset$; $1 = \{0\}$; $2 = \{0,1\} = \{\emptyset, \{\emptyset\}\}$; $3 = \{0,1,2\}$; $4 = \{0,1,2,3\}$,...

Cada número natural sería el conjunto constituido por todos los anteriormente definidos.

Intuitivamente el sucesor de un número natural es otro número con una unidad más, lo cual dentro de las ideas que estamos tratando de plasmar. significa que el sucesor de un natural es un conjunto con un elemento más: una manera de formar a partir de un conjunto dado A otro con un elemento más, es agregar el mismo A como elemento; le llamaremos "el sucesor de A" y lo notaremos A^+.

DEFINICIÓN 1. $A^+ = A \cup \{A\}$

El conjunto sucesor de A posee un elemento más que A si y sólo si $A \notin A$; aún cuando en este momento nos es imposible probar que $(\forall A)(A \notin A)$, más adelante demostraremos que todos los números naturales poseen esta propiedad; por ahora nos conformamos con lanzarle al lector el reto de tratar de idearse sin violar los axiomas dados, un conjunto que no cumpla esta propiedad.

Observemos que con la construcción sugerida de los naturales, cada uno

de ellos es el sucesor del anterior en el sentido de la definición 1:

$$0^+ = 0 \cup \{0\} = \emptyset \cup \{0\} = \{0\} = 1$$
$$1^+ = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0,1\} = 2$$
$$2^+ = 2 \cup \{2\} = \{0,1\} \cup \{2\} = \{0,1,2\} = 3, \quad \text{etc.},$$

pudiéndose continuar indefinidamente el proceso de formar el sucesor; puesto que en esta forma para definir un natural necesitamos haber definido previamente a todos los anteriores, para salvar la objeción a), debemos hallar un método de producir todos los naturales a la vez. Un conjunto que contenga a todos los naturales necesariamente es infinito; como estamos físicamente imposibilitados para construir conjuntos infinitos elemento por elemento, no nos queda otro remedio que introducir un nuevo axioma que nos garantice la existencia de tales conjuntos.

Depués de la motivación intuitiva precedente, construyamos formalmente los números naturales.

DEFINICIÓN 2. *Un conjunto se llama* inductivo *si:*
(i) *El conjunto vacío es elemento de él y*
(ii) *El sucesor de todo elemento de él también pertenece a él*

En el lenguaje conjuntista sería:
A es inductivo $\Longleftrightarrow$ (i) $\emptyset \in A$ y $(ii)(\forall X)(X \in A \longrightarrow X^+ \in A)$

Según las ideas expuestas, un conjunto inductivo es infinito; de ahí el nombre de nuestro próximo axioma:

A7 - Axioma del infinito

Existe al menos un conjunto inductivo.
En el simbolismo conjuntista sería

$$(\exists A)(\emptyset \in A \wedge (\forall X)(X \in A \longrightarrow X^+ \in A)).$$

De la simple definición 2 se obtiene el resultado siguiente:

PROPOSICIÓN 1. *La intersección de una colección no vacía de conjuntos inductivos, es un conjunto inductivo.*

Demostración. Sea C una colección no vacía de conjuntos inductivos; $\emptyset \in B$ para todo B de C, luego $\emptyset \in \bigcap_{B \in C} B$. Sea $X \in \bigcap_{B \in C} B$; se tiene que $X \in B$ para todo B en C y siendo todo B inductivo, también X^+ está en B (para todo B en C), luego $X^+ \in \bigcap_{B \in C} B$. □

Tomemos un conjunto inductivo cualquiera M (su existencia está garantizada por A7) y consideremos la colección $\mathfrak{I}$ de todos los subconjuntos inductivos de M (se obtiene separando de $\mathcal{P}(M)$ aquellos X que cumplen la condición "X es inductivo"). Siendo $M \subseteq M$, se tiene que $M \in \mathfrak{I}$, de modo que $\mathfrak{I}$ no es vacía. La proposición 1 implica que $\mathbb{N}_M = \bigcap_{B \in \mathfrak{I}} B$ es un conjunto inductivo.

PROPOSICIÓN 2. $(\forall A)(A$ es inductivo $\longrightarrow \mathbb{N}_M \subseteq A)$

Demostración. Sea A inductivo; por la proposición 1, $A \cap M$ es inductivo y como $A \cap M \subseteq M$, entonces $A \cap M$ pertenece a la colección $\mathfrak{I}$ de los subconjuntos inductivos de M; siendo $\bigcap_{B \in \mathfrak{I}} B$ subconjunto de todo conjunto de $\mathfrak{I}$, se tiene que $\mathbb{N}_M = \bigcap_{B \in \mathfrak{I}} B \subseteq A \cap M$ y como $A \cap M \subseteq A$, necesariamente $\mathbb{N}_M \subseteq A$. □

PROPOSICIÓN 3. *El conjunto* $\mathbb{N}_M$ *no depende de* M.

Demostración. Si M' fuese otro conjunto inductivo e $\mathfrak{I}'$ fuese la colección de los subconjuntos inductivos de M' y tomásemos $\mathbb{N}_{M'} = \bigcap_{B \in \mathfrak{I}'} B$, entonces $\mathbb{N}_{M'}$ también sería inductivo y por la proposición 2 se tendría $\mathbb{N}_M \subseteq \mathbb{N}_{M'}$, pero para $\mathbb{N}_{M'}$, también se podría igualmente demostrar la proposición 2 de modo que en particular $\mathbb{N}_{M'}$, sería subconjunto del conjunto inductivo $\mathbb{N}_M$, concluyéndose que $\mathbb{N}_M = \mathbb{N}_{M'}$. □

DEFINICIÓN 3. *Al conjunto* $\mathbb{N}_M = \mathbb{N}_{M'}$, *le notaremos simplemente por* $\mathbb{N}$ *y le llamaremos* el conjunto de los números naturales. *Un elemento de* $\mathbb{N}$ *se llamará un número natural.*

TEOREMA 1. *El conjunto* $\mathbb{N}$ *de los naturales es (respecto de la contenencia) el* mínimo conjunto inductivo, *es decir*
$(\forall S)$ (S *es inductivo* $\longrightarrow \mathbb{N} \subseteq S$).

Demostración. Es un corolario inmediato de la proposición 2 y de la definición 3. □

Este teorema realmente caracteriza al conjunto de los números naturales; para convencernos aún más que en verdad el $\mathbb{N}$ acabado de construir es el mismo conjunto de los naturales que conocíamos desde la escuela primaria, vamos a establecer ciertas propiedades un tanto peculiares que usaremos para finalmente demostrar que nuestros "naturales" satisfacen los cinco axiomas de Peano. Sus demostraciones ilustran una clase de prueba seguramente conocida por el lector: por inducción matemática.

PROPOSICIÓN 4. *Ningún número natural es subconjunto de alguno de sus elementos.*

Demostración. Sea S el conjunto de todos los números naturales que cumplen la propiedad dada, es decir,

$$S = \{n \in \mathbb{N} \mid (\forall X)(X \in n \longrightarrow \neg(n \subseteq X))\} \qquad (\alpha)$$

(o sea, si $X \in n$, entonces n no es subconjunto de X). Como queremos probar que todos los números naturales cumplen dicha propiedad, debemos demostrar que $S = \mathbb{N}$; siendo $S \subseteq \mathbb{N}$ por definición de S, bastará con establecer que $\mathbb{N} \subseteq S$, para lo cual, según el teorema 1, será suficiente probar que S es un conjunto inductivo. En efecto: Como $0 = \emptyset$ no posee elementos, entonces cero no puede ser subconjunto de alguno de sus elementos (o en (α) la implicación $X \in \emptyset \longrightarrow \neg(\emptyset \subseteq X)$ es verdadera para cualquier X por tener antecedente falso), con lo cual queda probada la condición (i) de la definición 2.

Demostraremos ahora que cualquiera sea n, $n \in S \longrightarrow n^+ \in S$.

Sea $n \in S$; como $n \subseteq n$, entonces $n \notin n$ (ya que si $n \in n$, sería n subconjunto de uno de sus elementos, el mismo n, contrario a la hipótesis $n \in S$); estando n en n^+ ($n^+ = n \cup \{n\}$) y no en n se concluye que n^+ no es subconjunto de n. Sea ahora x un elemento de n; por hipótesis $n \in S$, así que n no es subconjunto de x y menos aún lo será n^+ ya que $n^+ \supseteq n$.

Concluimos que si $x \in \{n\} \cup n = n^+$, entonces n^+ no es subconjunto de x, luego $n^+ \in S$, quedando probada la condición (ii) de la definición 2 y con ello la proposición 4. □

TEOREMA 2. *Ningún número natural es elemento de sí mismo, es decir* $(\forall n \in \mathbb{N})(n \notin n)$.

Demostración. Es una consecuencia inmediata de la proposición anterior, ya que si existiese un natural n tal que $n \in n$, entonces como $n \subseteq n$, se tendría que n sería subconjunto de uno de sus elementos, contrario a la proposición 4. □

Hemos probado así que efectivamente n^+ posee un elemento más que n, ya que $n \in n^+ \wedge n \notin n$.

COROLARIO 1. *n es subconjunto propio de n^+.*

Una propiedad bastante visible del hecho de que al construir los naturales resulta $\emptyset = 0$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, $4 = \{0, 1, 2, 3\}$, etc., es la siguiente:

PROPOSICIÓN 5. *Todo elemento de un número natural es un subconjunto propio de dicho natural.*

Demostración. Como antes, sea S el subconjunto de $\mathbb{N}$ formado por todos aquellos números naturales que poseen la propiedad enunciada, es decir, $S = \{n \in \mathbb{N} \mid (\forall X)(X \in n \longrightarrow X \subset n)\}$. Nuevamente debemos probar que S es inductivo. Como no existe un elemento en $\emptyset = 0$ que no sea subconjunto propio de $\emptyset$, se tiene que $0 = \emptyset \in S$. Supongamos que $n \in S$; sea $x \in n^+ = n \cup \{n\}$; $x \in n$ ó $x = n$; en el segundo caso $x = n \subset n^+$ (corolario del teorema 2); en el primer caso, estando n en S, se tedrá $x \subset n$ y como $n \subset n^+$, entonces $x \subset n^+$. Se concluye $n^+ \in S$ y con ello que S es inductivo y en consecuencia $\mathbb{N} \subseteq S$ y siendo $S \subseteq \mathbb{N}$, se obtiene la igualdad, quedando demostrado lo propuesto. □

PROPOSICIÓN 6. *La relación "$\in$" de pertenencia es transitiva en* $\mathbb{N}$.

Demostración. Sea $x \in n \wedge n \in m$; después de la proposición 5 se concluye $x \in n \wedge n \subset m$, luego $x \in m$. □

TEOREMA 3. *El conjunto* $\mathbb{N}$ *satisface los cinco axiomas de Peano.*

Demostración. Los axiomas N_1 y N_2 en conjunto son la simple fomulación de que $\mathbb{N}$ es inductivo y N_3 se deduce del hecho de ser $\mathbb{N}$ el mínimo conjunto inductivo; repitámoslo una vez más:

Si $S \subseteq \mathbb{N}$ tal que (i) $0 \in S$ y (ii) $(\forall n)(n \in S \longrightarrow n^+ \in S)$, también S es inductivo y siendo $\mathbb{N}$ el mínimo conjunto inductivo, $\mathbb{N} \subseteq S$. Concluimos que $S = \mathbb{N}$.

Esta propiedad se conoce con el nombre de *axioma de inducción* o a veces *principio de inducción, primera forma.*

El axioma N_4 también se cumple de manera inmediata: Como $n \notin \emptyset$ y $n \in n^+$ para todo n, entonces $\emptyset \neq n^+$ para todo n, así que no existe un natural del cual sea cero el sucesor.

Probemos N_5: Supongamos que $n^+ = m^+$.

Como $n \in n^+ = m^+ = m \cup \{m\}$, se sigue $(n \in m) \vee (n = m)$. Análogamente $m \in m^+ = n^+ = n \cup \{n\}$, luego $(m \in n) \vee (m = n)$. Resumiendo, $(n \in m \vee n = m) \wedge (m \in n \vee m = n)$, lo cual equivale a $(n \in m \wedge m \in n) \vee (n \in m \wedge m = n) \vee (n = m \wedge m \in n) \vee (n = m \wedge m = n)$.

La primera posibilidad no puede cumplirse porque la transitividad de la pertenencia implicaría $n \in n$, contradictorio con el teorema 2; tampoco pueden tenerse la segunda ni la tercera porque también conducirían a la contradicción $n \in n$; necesariamente se deberá cumplir la última $n = m$, probándose N_5 y con ello el teorema. □

Ejercicios

1. Simbolicemos con $N(x)$ al predicado unario "x es un número natural", por $S(x)$ a "el siguiente de x" (aquí S es una función u operación unaria), por 0 a la constante cero y por "$\in$" a la pertenencia de la teoría de conjuntos. En el lenguaje resultante al agregar los cuantificadores y los símbolos lógicos, enuncie los axiomas de Peano.

2. "Demuestre" que $\{A \mid A \approx \{a,b,c\}\} = \{A \mid A \approx \{\triangle, *, \square\}\}$.

3. Pruebe que para cualquier conjunto A se tiene que $A \in A^+$ y $A \subseteq A^+$.

4. Demuestre usando el axioma de inducción que

$$(\forall n \in \mathbb{N})(n \in m \longrightarrow (n^+ \in m \quad \veebar \quad n^+ = m)).$$

Recuerde que "$\veebar$" simboliza el *o* exclusivo.

5. Agregando a los axiomas $A1$ a $A6$ el siguiente

$$\#(A) = \#(B) \Leftrightarrow A \approx B,$$

pruebe que $\#(\mathbb{N}) = \#(\mathbb{Z})$ y que

$$\#(\{x \in \mathbb{R} \mid 0 < x < 1\}) = \#(\{x \in \mathbb{R} \mid a < x < b\}),$$

siendo a, b reales cualquiera con $a < b$.

6. Al comenzar el capítulo III dimos una motivación para hacer ver que el orden total de un conjunto finito puede expresarse en términos de conjuntos, habiéndose llegado a definir la pareja ordenada en la forma $(a,b) = \{\{a\},\{a,b\}\}$. Y la cuádrupla como

$$(a,b,c,d) = \{\{a\},\{a,b\},\{a,b,c\},\{a,b,c,d\}\}.$$

El ejercicio 4 de la sección 1 del capítulo III debió conducir a la siguiente definición de tripla

$$(a,b,c) = \{\{a\},\{a,b\},\{a,b,c\}\}.$$

El Dr. Carlos E. Vasco profesor titular de la Universidad Nacional de Colombia, propuso (ver [12]) la extensión de las definiciones anteriores:

$$(a_1) = \{\{a_1\}\} \quad ; \quad (a_1,a_2) = \{\{a_1\},\{a_1,a_2\}\} \quad \text{y}$$

$$(a_1,a_2,\cdots,a_n) = \{\{a_1\},\{a_1,a_2\},\cdots,\{a_1,a_2,\cdots,a_n\}\}$$

cualquiera sea $n \geq 1$.

Como lo hicimos notar, esta definición de n-pla lleva implícita la condición de que todos los elementos son distintos.

(a) Compruebe que con la anterior definición

$$(0,2,2) = (0,2,0) = (0,0,2) \qquad \text{y que}$$

$$(0,2,0,2) = (0,0,2,2) = (0,0,0,2) = (0,2,2,2)$$

con lo cual falla la propiedad fundamental de la n-pla.

(b) Verifique que

$$(0,2,0,2) = (0,2,0) = (0,2)$$

existiendo el colapso de una cuarteta a una tripla y aún a una dupla, defecto gravísimo que no permitiría definir coherentemente el número de coordenadas, ni la longitud de una sucesión finita, ni las proyecciones, entre otras cosas.

7) Los ejercicios 5 y 6 de la sección 1 del capítulo III tuvieron por finalidad dar la definición usual de n-pla, muy diferente a la del ejercicio anterior:

$$(a_1,a_2) = \{\{a_1\},\{a_1,a_2\}\},$$
$$(a_1,a_2,a_3) = ((a_1,a_2),a_3) \quad \text{y para } n \geq 3,$$
$$\vdots$$
$$(a_1,a_2,\cdots,a_n,a_{n+1}) = ((a_1,a_2,\cdots,a_n),a_{n+1}),$$

habiéndose demostrado que $(a_1,a_2,\cdots,a_n) = (b_1,b_2,\cdots,b_n)$ si y sólo si $a_i = b_i$ para todo $i = 1,2,\cdots,n$. El mismo profesor Vasco descubrió que también esta vez puede presentarse el colapso si se usa otra "copia conjuntista" de los naturales: La idea de presentar los números por rayas

$$|, \quad ||, \quad |||, \quad ||||, \cdots$$

puede formalizarse contando paréntesis izquierdos:

$$0 = \emptyset, \quad 1 = \{\emptyset\}, \quad 2 = \{\{\emptyset\}\}, \quad 3 = \{\{\{\emptyset\}\}\}$$

o sea que $0 = \emptyset$ y $n+1 = \{n\}$ cualquiera sea n.

Esto equivale a definir el sucesor como $A^+ = \{A\}$.

(a) Compruebe que con esta definición de naturales se tendría $(0,0) = 2$ y que $(0,0,2) = (2,2)$.

(b) Consultar en [13] la propuesta hecha por el profesor Vasco para dar una definición de n-pla que no presente el problema del colapso, independientemente de la "copia conjuntista" de $\mathbb{N}$ que se use.

4.2 EL ORDEN DE LOS NATURALES

El raciocinio utilizado en las demostraciones de las proposiciones 4 y 5 anteriores es válido en una gran cantidad de situaciones análogas, por lo cual le queremos dar una forma un poco más ágil.

TEOREMA 4. (Principio de inducción - segunda forma). *Sea $p(n)$ una codición en n (f.b.f en la cual la variable n es libre) ; si*

(i) $p(0)$ *es verdadera y*

(ii) $p(n^+)$ *es verdadera cada vez que* $p(n)$ *lo es* (*es decir*, $(\forall n \in \mathbb{N})(p(n) \longrightarrow p(n^+))$).

Entonces $p(n)$ *es verdadera para todo número natural, es decir*, $(\forall n \in \mathbb{N})(p(n))$.

Demostración. Al igual que antes, sea $S = \{n \in \mathbb{N} \mid p(n) \text{ es verdadera}\}$ Como $p(0)$ es verdadera, $0 \in S$.

Si $n \in S$, $p(n)$ es verdadera, lo cual junto con la hipótesis permite concluir que $p(n^+)$ es verdadera, o sea que $n^+ \in S$. En consecuencia S es inductivo, luego $S = \mathbb{N}$, lo cual es equivalente a $(\forall n \in \mathbb{N})(p(n))$. □

PROPOSICIÓN 7. *Cero es elemento de todo número natural distinto de cero, o sea*

$$(\forall n \in \mathbb{N})(n \neq 0 \longrightarrow 0 \in n)$$

Demostración. Por inducción: sea $p(n)$ la implicación

$$n \neq 0 \longrightarrow 0 \in n \quad .$$

(i) $p(0)$ es trivialmente válido ya que tanto el antecedente como el consecuente de

$$0 \neq 0 \longrightarrow 0 \in 0$$

son falsos.

Siendo $1 = 0^+ = \{0\}$, es evidente que $0 \in 1$, de manera que también vale $p(1)$.

(ii) Supongamos que $p(n)$ es verdadera. Si $n = 0$, entonces $p(n^+) = p(0^+) = p(1)$ también es cierto. Sea $n \neq 0$; por hipótesis de inducción $n \neq 0 \longrightarrow 0 \in n$ y aplicando modus ponens, $0 \in n$; como $n \in n^+$ y la

pertenencia es transitiva en $\mathbb{N}$ (prop. 6), se deduce que $0 \in n^+$, o sea que $p(n^+)$ también es verdadera.

La prueba se sigue del principio de inducción, segunda forma.

□

PROPOSICIÓN 8. $(\forall m)(\forall n)(n \in m \to ((n^+ \in m) \veebar (n^+ = m)))$.

Aun cuando el "o" del consecuente es exclusivo, basta probar la proposición para el caso en el que el "o" sea inclusivo, puesto que si $n^+ \in m \wedge n^+ = m$, se tendría la contradicción $n^+ \in n^+$.

La demostración la haremos por inducción sobre m, lo cual significa que en este caso se debe tomar como $\varphi(m)$:

$$(\forall n)(n \in m \longrightarrow (n^+ \in m \vee n^+ = m))$$

(i) $\varphi(0)$ es cierta porque el antecedente de la implicación es falso cualquiera sea n, puesto que $m = 0 = \emptyset$.

(ii) Supongamos que la propiedad vale para m y demostremos que también es cierta para m^+, es decir que

$$(n \in m^+) \longrightarrow (n^+ \in m^+ \vee n^+ = m^+) \quad .$$

Si $n \in m^+ = m \cup \{m\}$, debe tenerse $n \in m \vee n = m$; en el primer caso, como la propiedad vale para m, se tiene que $n^+ \in m \vee n^+ = m$, lo cual implica $n^+ \in m^+$ ya que $m \subseteq m^+$ y $m \in m^+$. En el segundo caso $n = m$, luego $n^+ = m^+$, quedando demostrado.

PROPOSICIÓN 9. $(\forall n, m \in \mathbb{N})(\neg(n \in m \wedge m \in n))$.

Demostración. Si sucediese que $n \in m \wedge m \in n$ para algún par de naturales, la transitividad de la pertenencia en $\mathbb{N}$ implicaría $n \in n$ contradictorio con el teorema 2, de modo que sean cuales fuesen los naturales n y m, se cumple $\neg(n \in m \wedge m \in n)$. □

La proposición anterior y la transitividad de la pertenencia en $\mathbb{N}$ significan que "$\in$" cumple en $\mathbb{N}$ con las condiciones de una relación de orden estricto, de modo que sin más demora establecemos la siguiente

DEFINICIÓN 4. *Sean n, m números naturales cualesquiera; $n < m$ significa $n \in m$; y $n \leq m$ significa $n < m \vee n = m$.*

Realmente este "o" es exclusivo porque

$$(n < m \wedge n = m) \longleftrightarrow (n \in m \wedge m = n) \quad \text{siguiéndose } n \in n \ ,$$

lo cual es contradictorio.

Según lo dicho, automáticamente "$\leq$" resulta ser una relación de orden en $\mathbb{N}$, precisamente el orden usual de $\mathbb{N}$.

PROPOSICIÓN 10. *Ley de tricotomía.*

$$(\forall n, m \in \mathbb{N})[(n = m) \veebar (n < m) \veebar (m < n)]$$

En español: para n, m naturales cualesquiera, siempre se cumple exactamente una de las relaciones $n = m, \quad n < m, \quad m < n$.

Demostración. Es imposible que se cumplan simultáneamente dos cualesquiera de las relaciones dadas, ya que se tendría una de las contradicciones $n \in n$ o $(n \in m \wedge m \in n)$. Por consiguiente basta demostrar que si $n \neq m$ entonces $n < m \vee m < n$, lo cual después de la definición 4 se traduce en $n \neq m \longrightarrow n \in m \vee m \in n$, cualesquiera sean n y m. Demostrémoslo por inducción sobre m.

(i) Cuando $m = 0$ la propiedad se cumple por la ya probada proposición 7: $(\forall n \in \mathbb{N})(n \neq 0 \longrightarrow 0 \in n)$.

(ii) Supongamos que la propiedad vale para m y demostrémosla para m^+. Sea $n \neq m^+$; si $n = m$, entonces $n \in m^+$ ya que $m \in m^+$. Si $n \neq m$, la hipótesis de inducción nos permite afirmar (a) $n \in m$ o (b) $m \in n$. En el caso (a), como $m \in m^+$ se concluye que $n \in m^+$. En el caso (b) la proposicipon 8 nos permite afirmar $m^+ \in n$ o $m^+ = n$. pero $n \neq m^+$ por hipótesis, luego $m^+ \in n$.

□

PROPOSICIÓN 11. *El orden usual de $\mathbb{N}$ es total.*

Demostración. Es una consecuencia evidente de la ley de tricotomía. □

PROPOSICIÓN 12. $n < m \Leftrightarrow n^+ < m^+$

Demostración. Si $n < m$, por la definición 4 y la proposición 8 concluimos que $n^+ \leq m$ y como $m < m^+$, por transitividad se obtiene $n^+ < m^+$.

El recíproco se prueba usando la ley de tricotomía y la parte ya demostrada. □

La proposición 12 nos dice en particular que la función $S : \mathbb{N} \longrightarrow \mathbb{N}$ dada por $S(n) = n^+$ es estrictamente creciente.

Finalmente probaremos el resultado más fuerte sobre el orden de $\mathbb{N}$:

TEOREMA 5. *El orden usual de $\mathbb{N}$ es un buen orden.*

Demostración. La haremos por contradicción. Supongamos que la propiedad no se cumple; existe entonces un subconjunto *no vacío* A de $\mathbb{N}$ sin primer elemento. Sea S el subconjunto de $\mathbb{N}$ constituido por aquellos naturales menores estrictamente que todos los elementos de A:

$$S = \{n \in \mathbb{N} \mid (\forall k \in A)(n < k)\} \quad .$$

La proposición queda demostrada si llegamos a probar que S es inductivo, ya que se tendría $S = \mathbb{N}$ y como consecuencia la contradicción $A = \emptyset$.

(i) La proposición 7 significa $0 < n$ para todo natural $n \neq 0$, de modo que el cero es el primer elemento de $\mathbb{N}$. Si $0 \in A$, cero sería también el primer elemento de A, pero como A no posee primer elemento, $0 \notin A$ y por consiguiente $0 \in S$.

(ii) En vez de probar directamente que $n \in S \longrightarrow n^+ \in S$, demostraremos $n^+ \notin S \longrightarrow n \notin S$, equivalente a lo anterior. Si $n^+ \notin S$, existe k en A tal que $k \leq n^+$. Como k no es el primer elemento de A (A no posee primer elemento) y el orden es total, existe m en A tal que $m < k$; de la proposición 8, $m^+ \leq k$ y por transitividad, $m^+ \leq n^+$, lo cual por la proposición 12 implica $m \leq n$ y en consecuencia $n \notin S$.

□

Los ejercicios 1. a 4. que aparecen al final de esta sección tienen por objeto proponer una demostración alternativa de la buena ordenación de $\mathbb{N}$.

Terminamos estableciendo algunas propiedades de los conjuntos finitos.

PROPOSICIÓN 13. *Todo subconjunto propio de un número natural es equipotente con un natural menor.*

Demostración. Lo haremos por inducción;

(i) Para 0 como es igual a $\emptyset$, se cumple vaciamente la propiedad ya que no posee subconjuntos propios.

(ii) Supongamos la propiedad válida para n. Sea E un subconjunto propio de $n^+ = n \cup \{n\}$,

(a) Si $n \notin E$, entonces $E = n$ ó, E es un subconjunto propio de n ; cuando $E = n$, $E \approx n$; cuando E es un subconjunto propio de n, por hipótesis de inducción E será equipotente con un natural menor que n y por consiguiente menor que n^+.

(b) Si $n \in E$, no se puede tener $E - \{n\} = n$ porque entonces $E = n \cup \{n\} = n^+$, contrario a la hipótesis de ser E un subconjunto propio de n^+. Entonces $E - \{n\}$ es un subconjunto propio de n y por hipótesis de inducción, existe $k < n$ tal que $E - \{n\} \approx k$, luego $E \approx k^+$ y $k^+ \leq n < n^+$, quedando demostrado.

□

PROPOSICIÓN 14. *Ningún natural es equipotente con alguno de sus subconjuntos propios.*

Demostración. Por inducción.

(i) La propiedad se cumple vaciamente para $0 = \emptyset$ por no poseer subconjuntos propios. Como en el teorema 5, demostraremos $\neg(p(n^+)) \longrightarrow \neg(p(n))$; supongamos $\neg(p(n^+))$; existe A un subconjunto propio de n^+. equipotente con n^+; sea $f : n^+ \longrightarrow A$ la biyección que establece la equipotencia;

(a) Si $n \notin A$, A es subconjunto de n y la restricción $f|_n : \{0, 1, 2 \cdots, n-1\} \longrightarrow A' = A - \{f(n)\}$ es una biyección entre n y el subconjunto propio A' de n, así que $\neg p(n)$.

(b) Si $n \in A$, como $n^+ \approx A$, entonces $n = n^+ - \{n\} \approx A - \{n\}$ siendo éste último subconjunto propio de n ya que A lo es de n^+, luego $\neg p(n)$.

□

COROLARIO 2. *Dos naturales son equipotentes si y solo si son iguales.*

Demostración. Si $m = n$, entonces $m \approx n$ por ser todo conjunto equipotente consigo mismo. Veamos que $(m \approx m) \rightarrow (m = n)$: Supongamos que $m \approx n$: por tricotomía, $(m = n) \underline{\vee} (m \in n) \underline{\vee} (n \in m)$. Pero las dos últimas posibilidades no pueden darse porque como $m \approx n$, se tendría un natural equipotente con uno de sus elementos, o sea con uno de sus subconjuntos propios (según la proposición 5). En consecuencia se tendrá $m = n$. □

¿Cuándo un conjunto es finito? Desde temprana edad nuestra intuición nos dice que un conjunto es finito si le podemos contar sus elementos; pero hacer esto es ir asignando a sus elementos los números $1, 2, 3 \cdots$ hasta un

cierto n, en cuyo caso decimos que el conjunto es finito y posee n elementos. Lo anterior equivale a afirmar que A es finito y posee n elementos si existe una biyección entre A y el conjunto $\{1, 2, \cdots, n\}$, o lo que es lo mismo, si existe una biyeción entre A y $\{0, 1, \cdots, n-1\}$, como si contásemos desde cero; ésta será precisamente nuestra definición oficial.

DEFINICIÓN 5. *Un conjunto se llama* finito *si es equipotente con algún número natural. Es decir, A es finito si y sólo si existe un natural n tal que $A \approx \{0, 1, \cdots, n-1\} = n$.*

Dicho natural es único, ya que si existiese también m tal que $A \approx m$, la transitividad de la equipotencia implicaría $m \approx n$, lo cual equivale (según corolario de la proposición 14) a $m = n$.

Usamos la notación $n = \#(A)$ para designar a este único natural con el cual A es equipotente y decimos que A posee n elementos o que el cardinal de A es n.

Un conjunto se llama *infinito* si no es finito.

La propiedad siguiente caracteriza a los conjuntos finitos:

PROPOSICIÓN 15. *Ningún conjunto finito es equipotente con alguno de sus subconjuntos propios.*

Demostración. Por contradicción: si existiera un conjunto finito A equipotente con uno de sus subconjuntos propios, digamos con E, como A es finito, existen $n \in \mathbb{N}$ y $f\colon A \longrightarrow n$ biyectiva; pero $E \approx f(E)$, luego $n \approx A \approx E \approx f(E)$ o sea $n \approx f(E)$ y $f(E)$ es un subconjunto propio de n, ya que E lo es de A, contrario a la proposición 14. □

PROPOSICIÓN 16. *Todo subconjunto de un conjunto finito es también finito.*

Demostración. Sea A un conjunto finito y sea E un subconjunto propio de A (si $E = A$, E es finito); existe $f\colon A \longrightarrow n$ biyectiva, luego $E \approx f(E)$ y este último es un subconjunto propio de n, y por la proposición 13, $f(E)$ es equipotente con un natural k menor que n, luego $E \approx f(E) \approx k$ siendo E finito y además $\#(E) = k < \#(A)$. □

COROLARIO 3. *Si $A \subseteq B$ y B es finito, entonces A también es finito y $\#(A) \leq \#(B)$.*

Su demostración está hecha dentro de la misma prueba de la proposición anterior.

Ejercicios

1. Demuestre por inducción que todo subconjunto no vacío de un número natural, tiene primer elemento.
2. Sea A un subconjunto no vacío de $\mathbb{N}$. Pruebe que si $n \in A$ y $n \cap A$ es vacío, entonces n es el primer elemento de A.
3. Sea A un subconjunto no vacío de $\mathbb{N}$, $A \neq \{0\}$. Pruebe que si existe n en A tal que $n \cap A \neq \emptyset$, entonces como por el ejercicio 1, $n \cap A$ tiene primer elemento n_o en n, también n_o es el primer elemento de A.
4. Use los resultados de los tres ejercicios anteriores para demostrar que $\mathbb{N}$ con el orden usual es bien ordenado.
5. Demuestre el "principio de inducción, tercera forma": Sea $p(k)$ una condición en k, con esta variable libre tomando valores en $\mathbb{N}$.

   Si (i) $p(k_0)$ es verdadera y (ii) $(\forall k \geq k_0)(p(k) \longrightarrow p(k^+))$ entonces $(\forall k \geq k_0)(p(k))$, es decir, $P(k)$ es verdadera para todo $k \geq k_0$.

   Ayuda: Demuestre que el conjunto

   $$S = \{0, 1, 2, \cdots, k_0 - 1\} \cup \{k \in \mathbb{N} \mid p(k)\}$$

   es inductivo.
6. Pruebe que las tres formas anteriormente dadas del principio de inducción son todas equivalentes entre sí.
7. Demuestre que si un conjunto es equipotente con alguno de sus subconjuntos propios, entonces es infinito. Use este resultado y el axioma 5 de Peano para probar que $\mathbb{N}$ es infinito.
8. Pruebe que $\mathbb{N} \notin \mathbb{N}$.

   Ayuda: Use el ejercicio anterior y la proposición 14.
9. Demuestre que $(\forall n \in \mathbb{N})(n \neq 0 \longrightarrow (\exists k \in \mathbb{N})(n = k^+))$.
10. Pruebe por inducción que todo natural es un subconjunto de $\mathbb{N}$.
11. Demuestre que ningún natural puede ser equipotente con $\mathbb{N}$.

    Ayuda: Si $n \approx \mathbb{N}$, entonces $n^+ \approx \mathbb{N}^+ \approx \mathbb{N} \approx n$.

4.3 INDUCCIÓN MATEMÁTICA

En las tres formas dadas del principio de inducción, cuando se desea probar que una propiedad vale para n^+, sólo se puede usar como hipótesis (de inducción) el que la propiedad es cierta para un primer elemento y para el predecesor inmediato de n^+, esto es, para n; sin embargo, es muy útil en algunos casos una versión del principio de inducción con una hipótesis más fuerte en la cual para demostrar que una propiedad vale para n^+, se pueda usar como hipótesis el que la propiedad vale para todos sus predecesores rigurosos; antes de enunciarla introduciremos un concepto que facilita el tratamiento y permite su generalización.

DEFINICIÓN 6. *Sea $\leq$ una relación de orden total en un conjunto A y sea $<$ su orden estricto correspondiente; para cada b en A, llamaremos segmento inicial determinado por b (notado $\sigma(b)$) al conjunto de todos los elementos de A que preceden rigurosamente a b, es decir ,*

$$\sigma(b) = \{x \in A \mid x < b\}$$

TEOREMA 6. *Principio de inducción, 4a. forma:*
Si S es un subconjunto de $\mathbb{N}$ tal que $(\forall a \in \mathbb{N})(\sigma(a) \subseteq S \longrightarrow a \in S)$, entonces $S = \mathbb{N}$.

Por supuesto $\sigma(a) = \{x \in \mathbb{N} | x < a\}$, donde "$<$" es el orden usual estricto entre naturales.

El teorema significa exactamente lo que se quería: si S es un subconjunto de $\mathbb{N}$ tal que cada vez que *todos* los predecesores estrictos de un elemento están en S entonces el elemento también está es S, se debe cumplir que S es todo $\mathbb{N}$.

Demostración. Si $S \neq \mathbb{N}$, entonces $\mathbb{N} - S \neq \emptyset$ y como $\mathbb{N}$ es bien ordenado por el orden usual, existe primer elemento, digamos n_0, en $\mathbb{N} - S$. Luego si $x \in \mathbb{N}$ y $x < n_0$, necesariamente x está en S, o sea que $\sigma(n_0) \subseteq S$, luego por modus ponens aplicado a la hipótesis concluimos que $n_0 \in S$, lo cual es contradictorio ya que n_0 está en $\mathbb{N} - S$ (es su primer elemento). En consecuencia $S = \mathbb{N}$. □

Como corolario tenemos el resultado siguiente:

PROPOSICIÓN 17. Principio de inducción, 5a. forma: *Si $p(n)$ es una condición en n tal que*

(i) *$p(0)$ es cierto y*

(ii) $p(0) \wedge P(1) \wedge \cdots \wedge p(n) \longrightarrow p(n^+)$,

entonces $(\forall n \in \mathbb{N})(p(n))$.

Su demostración es inmediata aplicando el teorema anterior y se deja al lector como un sencillo ejercicio.

Estas dos últimas formas del principio de inducción pueden modificarse de modo que sirvan para hacer demostraciones por inducción en conjuntos bien ordenados cualesquiera.

TEOREMA 7. *Principio de inducción transfinita.*
Sea A un conjunto bien ordenado por $\leq$; si S es un subconjunto de A tal que

$$(\forall a \in A)(\sigma(a) \subseteq S \longrightarrow a \in S)$$

entonces $S = A$.

Se sobrentiende aquí que $\sigma(a) = \{x \in A \mid x < a\}$.

Demostración. Basta repetir el razonamiento usado en la prueba del teorema 6 : Si $A - S$ no fuese vacío, existiría un primer elemento x_0 en $A - S$ ya que la relación es de buen orden; entonces, si $x < x_0$, necesariamente $x \in S$, es decir $\sigma(x_0) \subseteq S$ y por hipótesis se deduce que $x_0 \in S$, lo cual es contradictorio con $x_0 \in A - S$, quedando demostrado el teorema. □

La diferencia principal del principio de inducción transfinita con el de inducción corriente no radica en que el segundo exige $0 \in S$ (ya que de $\sigma(0) = \emptyset \subseteq S$ se deduce que $0 \in S$) sino en que aquel no presupone la existencia del predecesor inmediato de todo elemento diferente del primero, pasando del conjunto de todos los predecesores estrictos de un elemento al elemento mismo, y no del predecesor inmediato al elemento; esta pequeña (en apariencia) diferencia es fundamental, ya que en muchos conjuntos bien ordenados no siempre existe el predecesor inmediato de todo elemento; por ejemplo si $A = \mathbb{N} \cup \{\mathbb{N}\} = \{0, 1, 2, \cdots, \mathbb{N}\}$, podemos ordenarlo bien con solo tomar como orden entre elementos de $\mathbb{N}$ el usual y definir $n < \mathbb{N}$ para todo n natural; aquí el elemento $\mathbb{N}$ de A no posee predecesor inmediato.

Este mismo ejemplo nos sirve para poner de presente que en general el principio de inducción transfinita no implica al principio de inducción, o sea que en general el principio de inducción y el de inducción transfinita no son equivalentes. Si $S = \mathbb{N} \subseteq A$, se cumple que

(i) $0 \in S$ y

(ii) $(\forall n \in A)(n \in S \longrightarrow n^+ \in S)$,

y sin embargo $S \neq A$.

Para $(\mathbb{N}, \leq)$ y los conjuntos bien ordenados cuyo orden es semejante al de $(\mathbb{N}, \leq)$, sí se tiene la equivalencia.

PROPOSICIÓN 18. *En $\mathbb{N}$ (con el orden usual) el principio de inducción y el de inducción transfinita, son equivalentes.*

En el teorema 5 se demostró que el principio de inducción (PI) implica el buen orden de $\mathbb{N}$ (B.O). En el teorema 6 se probó que a su vez B.O implica el principio de inducción transfinita (PIT), de modo que sólo nos resta demostrar que esto último implica PI para así establecer la equivalencia en $\mathbb{N}$ de estos tres enunciados. Veamos que en $\mathbb{N}$ con el orden usual, PIT $\longrightarrow$ PI. Supongamos que en $\mathbb{N}$ vale el principio de inducción transfinita. Sea $S \subseteq \mathbb{N}$ tal que

(i) $0 \in S$ y

(ii) $(\forall n \in \mathbb{N})(n \in S \longrightarrow n^+ \in S)$;

la demostración queda completa si podemos concluir que $S = \mathbb{N}$.
Veamos que se verifica que $(\forall n \in \mathbb{N})(\sigma(n) \subseteq S \longrightarrow n \in S)$:
Como por (i) $0 \in S$, entonces trivialmente $(\sigma(0) \subseteq S \longrightarrow 0 \in S)$. Supongamos que $n \neq 0$ y $\sigma(n) \subseteq S$. Puesto que $n \neq 0$, existe $k \in \mathbb{N}$ tal que $n = k^+$ ejercicio 9, sección anterior) de modo que $\sigma(n) = \sigma(k^+) \subseteq S$ y como $k < k^+$, entonces $k \in \sigma(k^+)$ o sea que $k \in S$ y por (ii), $n = k^+ \in S$.

Luego, en cualquier caso $\sigma(n) \subseteq S$ implica $n \in S$, así que el principio de inducción transfinita nos permite concluir que $S = \mathbb{N}$, quedando demostrado.

Sean X un conjunto no vacío y $f : X \longrightarrow X$ una función cualquiera. Tomemos un elemento a de X; hallemos $f(a)$; como $f(a) \in X$, podemos calcular $f(f(a))$; estando a su vez $f(f(a))$ en X, podemos obtener $f(f(f(a)))$; repitiendo el procedimiento cuantas veces queramos, formaremos:
$f(f(f(f(a)))), f(f(f(f(f(a))))), \ldots$

Lo anterior nos sugiere que podemos definir una función u de $\mathbb{N}$ en X, consistente en la aplicación repetida de la función f, tantas veces como el natural en el cual se calcula u; más explícitamente:

$$\begin{aligned} u(0) &= a \\ u(1) &= f(a) \\ u(2) &= f(f(a)) \\ u(3) &= f(f(f(a))) \\ &\vdots \end{aligned}$$

Obsérvese que tal función u queda "perfectamente determinada" con solo elegir $a = u(0)$; también nótese que

$$\begin{aligned} u(0) &= a \\ u(0^+) = u(1) &= f(a) = f(u(0)) \\ u(1^+) = u(2) &= f(f(a)) = f(u(1)) \\ u(2^+) = u(3) &= f(f(f(a))) = f(u(2)) \\ \vdots \qquad &\qquad \vdots \qquad\qquad \vdots \end{aligned}$$

lo cual hace ver que cualquiera sea $n \in \mathbb{N}$,

$$u(n^+) = f(u(n))$$

Los puntos suspensivos que hemos puesto anteriormente sugieren que la definición de la función u se puede continuar indefinidamente ("f se puede aplicar al elemento a cuantas veces queramos"), pero como deseamos que u tenga como dominio *todo* $\mathbb{N}$ y estando físicamente imposibilitados para definir $u(n)$ para cada número natural n (por ser $\mathbb{N}$ infinito), necesitamos de un teorema que nos garantice la existencia (y la unicidad) de una función u que cumpla las condiciones requeridas.

TEOREMA 8. *(Teorema de definición por recurrencia).*
Dados un conjunto X no vacío, una función f de X en X y un elemento a de X, existe una única función $u : \mathbb{N} \longrightarrow X$, tal que:

(1) $u(0) = a$

(2) $u(n^+) = f(u(n))$, *para todo* $n \in \mathbb{N}$.

Demostración. Siendo una función una relación especial, la idea a seguir consiste en hallar entre todas las relaciones de $\mathbb{N}$ en X (es decir, entre todos los subconjuntos de $\mathbb{N} \times X$) la relación más pequeña (con respecto a "$\subseteq$") que cumpla las condiciones (1) y (2) anteriores.

Sea C la colección de todos los subconjuntos R de $\mathbb{N} \times X$ tales que

(a) $(0,a) \in R$ y

(b) Si $(n,x) \in R$, entonces $(n^+, f(x)) \in R$.

C no es vacía ya que $\mathbb{N} \times X \in C$ y en consecuencia la intersección de C existe; sea $u = \bigcap_{R \in C} R$. Se sigue que u es la mínima relación de $\mathbb{N}$ en X que cumple (a) y (b), y posee dominio $\mathbb{N}$ (como se comprueba fácilmente por inducción).

Demostremos que u es una función; es suficiente probar que el conjunto S de todos los números naturales n para los cuales existe una única x en X tal que $(n,x) \in u$, es todo $\mathbb{N}$. Hagámoslo por inducción.

(i) Como $(0,a) \in u$, si $0 \notin S$, existiría $b \neq a$ tal que $(0,b) \in u$. Entonces $u' = u - \{(0,b)\}$ pertenecería a C, contrario al hecho de que u es la mínima relación de C. (Como $(0,b) \neq (0,a)$, entonces $(0,a) \in u'$; si $(n,x) \in u'$, $(n,x) \in u$ luego $(n^+, f(x)) \in u$ y como $(n^+, f(x)) \neq (0,b)$, entonces $(n^+, f(x)) \in u'$, concluyéndose que $u' \in C$).

(ii) Supongamos que $n \in S$; existe un único x en X tal que $(n,x) \in u$; se sigue que $(n^+, f(x)) \in u$. Si n^+ no estuviera en S, existiría $y \neq f(x)$ tal que $(n^+, y) \in u$. Al igual que antes, $\overline{u} = u - \{(n^+, y)\}$ estaría en C, contrario nuevamente al hecho de ser u la mínima relación de C. ($\overline{u} \in C$: $(0,a) \in \overline{u}$ ya que $(0,a) \in u$ y $(0,a) \neq (n^+, y)$. Si $(m,z) \in \overline{u}$, $(m,z) \in u$ y $(m^+, f(z)) \in u$; si $m = n$, entonces $z = x$ y $(m^+, f(z)) = (n^+, f(x)) \in \overline{u}$ ya que $y \neq f(x)$. Si $m \neq n$, entonces $(m^+, f(z)) \neq (n^+, y)$ así que $(m^+, f(z)) \in \overline{u}$, luego $\overline{u} \in C$).

□

Cuando usamos el teorema anterior para definir algo, decimos que lo hemos *definido por recurrencia*. Como ilustración verdaderamente provechosa definiremos por recurrencia en el próximo numeral las operaciones usuales entre naturales. Por ahora simplemente definamos por recurrencia b^n para un real b cualquiera: Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $(\forall x \in \mathbb{R})(f(x) = xb)$ y tomemos $a = 1$. Definamos $\mu : \mathbb{N} \longrightarrow \mathbb{R}$ mediante $\mu(0) = 1$ y $\mu(n^+) = f(\mu(n))$. Entonces

$$\mu(1) = \mu(0^+) = f(\mu(0)) = \mu(0)b = 1b = b$$
$$\mu(2) = \mu(1^+) = f(\mu(1)) = \mu(1)b = bb = b^2$$

y en general $\mu(n)$ será b^n. Como $\mu(0) = 1$ y $\mu(n^+) = f(\mu(n)) = \mu(n) \cdot b = b^n \cdot b$, se acostumbra dar esta definición en la forma

$$b^0 = 1 \quad \text{y} \quad b^{n+1} = b^n b$$

ya que en adelante n^+ será precisamente $n + 1$.

Ejercicios

1. Consideremos el siguiente subconjunto de $\mathbb{R}$:

$$A = \{-1/n \mid n \in \mathbb{N}^*\} \cup \{1/n \mid n \in \mathbb{N}^*\}$$

ordenado con el orden heredado de $\mathbb{R}$.

(a) ¿Es A bien ordenado?

(b) ¿Todo elemento de A posee sucesor inmediato?

(c) ¿Todo elemento de A posee predecesor inmediato?

2. Responda las mismas preguntas hechas en el ejercicio anterior para

$$B = \{1/n \mid n \in \mathbb{N}^*\} \cup \{1 + 1/n \mid n \in \mathbb{N}^*\}$$

3. Compruebe que para el orden usual de $\mathbb{N}$ se cumple que $\sigma(n) = n$, cualquiera sea el natural n.

4. Averigüe cuál es el teorema fundamental de la aritmética y compruebe que cuando se demuestra por inducción, se usa la quinta forma de dicho principio.

5. ¿Qué es una sucesión $x_0, x_1, x_2, x_3, \cdots$, de elementos de un conjunto X? No es otra cosa que una función $f : \mathbb{N} \longrightarrow X$ de la cual se han escrito solamente las imágenes, conservando claro está el orden de los naturales de donde provienen, o sea que se sobrentiende que $x_0 = f(0)$, $x_1 = f(1)$, y en general $x_n = f(n)$. Algunas veces se acostumbra usar una notación como $(x_n)_{n \in \mathbb{N}}$ para representar la función $\{(n, f(n) \mid n \in \mathbb{N}\}$. Obsérvese que debido a lo bien que conocemos $\mathbb{N}$, la función f queda perfectamente determinada en la forma anterior; por ejemplo $1, 1/2, 1/4, 1/8, 1/16, \cdots$ es simplemente la función $f : \mathbb{N} \longrightarrow \mathbb{R}$ tal que $f(0) = 1, f(1) = 1/2, f(2) = 1/4, \cdots, f(n) = 1/2^n, \cdots$

(a) Usando sólo los elementos del conjunto $\{0,1\}$, ¿Cuántas sucesiones finitas con a lo más tres términos pueden formarse?

¿Cuántas con a lo más 7 términos? ¿Cuántas con a lo más m términos?

(b) Defina tres sucesiones de números racionales no todos enteros, dando en cada caso explícitamente la función $h : \mathbb{N} \longrightarrow \mathbb{Q}$.

(c) Defina por recurrencia tres sucesiones de números reales no todos racionales, dando en cada caso la función $f : \mathbb{R} \longrightarrow \mathbb{R}$, el elemento a de $\mathbb{R}$, y calculando los cinco primeros términos de la función $\mu : \mathbb{N} \longrightarrow \mathbb{R}$ resultante.

(d) ¿Existe alguna diferencia entre la sucesión $x_0, x_1, x_2, \cdots$ y el conjunto $\{x_0, x_1, x_2, \cdots\} = \{x_n \mid n \in \mathbb{N}\}$?

6. Sea $f : [0, \infty) \longrightarrow [0, \infty)$ dada por $f(x) = \sqrt{1+x}$; definamos $\mu : \mathbb{N} \longrightarrow [0, \infty)$ mediante $\mu(0) = 2$ y $(\forall n)(\mu(n+1) = f(\mu(n)))$.

a) Halle los cinco primeros términos de la sucesión μ.

*(b) ¿Tenderá $\mu(n)$ a algún límite cuando $n \longrightarrow \infty$?

7. Podemos obtener un *principio de definición por recurrencia de segundo orden* de la forma siguiente:

Sean $f : X \times X \longrightarrow X$ y $a, b \in X$; entonces existe una única función $\mu : \mathbb{N} \longrightarrow X$ tal que

(i) $\mu(0) = a$

(ii) $\mu(1) = b$ y

(iii) $(\forall n \in \mathbb{N})(\mu(n+2) = f(\mu(n), \mu(n+1)))$.

Su demostración es en esencia similar a la del principio usual:

Sea C la colección de todos los subconjuntos R de $\mathbb{N} \times X$ tales que

(i) $(0, a) \in R$ (ii) $(1, b) \in R$ y

(iii) $[(n, x) \in R \wedge (n+1, y) \in R] \longrightarrow (n+2, f(x, y)) \in R$.

La función μ será la intersección de todas las R de C. Dejamos al lector la tarea de completar la demostración.

(a) Un ejemplo de aplicación es el siguiente: Si $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ es la suma de naturales, existe una única función $\mu : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $\mu(0) = 1$, $\mu(1) = 1$ y $\mu(n+2) = f(\mu(n), \mu(n+1)) = \mu(n) + \mu(n+1)$; se llama *la sucesión de Fibonacci*. Calcule los primeros quince términos de esta sucesión.

(b) Use este principio para definir dos sucesiones de números reales, dando los primeros cinco términos de cada una de ellas.

(c) Halle los diez primeros términos de la sucesión definida por $f(x, y) = (x + y)/2$, siendo $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$, cuando i) $a = 1$ y $b = 5$ o ii) $a = 5$ y $b = 1$.

8. Un tercer principio de definición por recurrencia que permite obtener sucesiones diferentes a las producidas con los otros dos principios, es el siguiente:

Dadas $f : \mathbb{N} \times X \longrightarrow X$ y $a \in X$, existe una única fución $\mu : \mathbb{N} \longrightarrow X$ tal que

i) $\mu(0) = a$ y

ii) $\forall n \in \mathbb{N}$, $\mu(n+1) = f(n, \mu(n))$.

Su demostración es similar a las de los dos principios anteriores y la dejamos como ejercicio.

Use este principio para definir recursivamente el factorial:

$$0! = 1 \quad y \quad n! = 1 \times 2 \times 3 \times \cdots \times n \quad \text{si } n \geq 1.$$

9. Use el principio que sea del caso para definir por recurrencia

(a) $2, 2^2, 2^{(2^2)}, 2^{(2^{(2^2)})}, \ldots$

(b)

$$a_n = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots\, 2 + \frac{1}{2}}}}$$

con $n+1$ doses

(c) $b_n = 1 + 2 + 3 + \cdots + n$

(d) $c_n = (5+1)(5+2)\cdots(5+n)$

*10) Si usamos repetidamente pero finitas veces el axioma del conjunto de partes, podemos formar

$$A,\ \mathcal{P}(A),\ (\mathcal{P}(\mathcal{P}(A))) = \mathcal{P}^2(A),\ (\mathcal{P}(\mathcal{P}(\mathcal{P}(A)))) = \mathcal{P}^3(A), \ldots$$

y en general, si n es un natural cualquiera, siempre podemos formar

$\mathcal{P}^n(A)$. ¿Podrá usarse algunos de los principios de definición por recurrencia para obtener una función μ de dominio $\mathbb{N}$ tal que

$\mu(0) = A$ y para todo n, $\mu(n+1) = \mathcal{P}(\mu(n))$?

*11) Análogamente, podemos usar el producto cartesiano para formar A, $A \times A = A^2$, $(A \times A) \times A = A^3, \ldots$ ¿Podrá utilizar alguno de los principios vistos para obtener una función η de dominio $\mathbb{N}$ tal que para todo $n \geq 1$, $\eta(n) = A \times A \times \cdots \times A$ (n veces A) ?

4.4 OPERACIONES ENTRE NATURALES.

El propósito de esta sección es definir por recurrencia adición, multiplicación y exponenciación en el conjunto de los números naturales, demostrar algunas de sus propiedades y proponer la prueba de otras, todo ello dentro del esquema conjuntista en el cual hemos venido trabajando.

La definición de adición la damos copiando la forma como los niños suman utilizando los dedos: $5 + 3 = ((5 + 1) + 1) + 1$; es decir que si sabemos sumar a un natural el número uno, podremos sumar a dicho natural cualquier otro. Realmente sí sabemos sumar el número uno:

$$m + 1 = m^+$$

y en consecuencia

$m+2 = (m^+)^+ = (m+1)+1$, $m+3 = (m+2)^+ = ((m+1)+1)+1$, etc. $\cdots$

En forma más rigurosa y oficial: En el teorema de definición por recurrencia, tomemos como $f : X = \mathbb{N} \longrightarrow \mathbb{N}$ la función que a cada natural hace corresponder su sucesor inmediato, esto es, $f(x) = x^+$ y elijamos para el papel de a en dicho teorema a un número natural m. Existe entonces una única función $S_m : \mathbb{N} \longrightarrow \mathbb{N}$ tal que

$$S_m(0) = m \quad \text{y} \quad S_m(n^+) = f(S_m(n)) = (S_m(n))^+$$

Disponiendo de una tal función S_m para cada número natural m, podemos definir la adición en $\mathbb{N}$ así:

$$m + n = S_m(n)$$

Realmente es la definición usual:

$$\begin{aligned}
m + 0 &= S_m(0) = m \\
m + 1 &= S_m(1) = S_m(0^+) = (S_m(0))^+ = m^+ \\
m + 2 &= S_m(2) = S_m(1^+) = (S_m(1))^+ = (m+1)^+ = (m+1) + 1 \\
m + 3 &= S_m(3) = S_m(2^+) = (S_m(2))^+ = ((m+1)+1)^+ \\
&= ((m+1)+1) + 1 \\
&\vdots
\end{aligned}$$

y en general $m + n$ será el resultado de sumar a m el número 1 ene veces.

Después de la segunda de las igualdades anteriores, en adelante procuraremos escribir $m+1$ en vez de m^+. Nótese que estamos usando el símbolo "+" entre dos naturales para indicar su adición y como superíndice para designar al sucesor; su doble significado sin embargo no da lugar a confusiones, de modo que lo conservaremos.

Demostraremos ahora las propiedades usuales de la adición de números naturales.

Propiedad Modulativa: $(\forall m \in \mathbb{N})(m + 0 = m = 0 + m)$

De la definición de adición $m + 0 = S_m(0) = m$, luego es suficiente probar que $0 + m = m$; lo haremos por inducción:

(i) Si $m = 0$: $0 + 0 = S_0(0) = 0$, siendo válido.

(ii) Supongamos que $0 + m = m$.

$$0 + m^+ = S_0(m^+) = (S_0(m))^+ = (0 + m)^+ = (m)^+,$$

siendo la hipótesis de inducción la justificación de la última igualdad de la cadena anterior.

De utilidad posterior es el siguiente

LEMA 1. $(\forall m)(\forall n)(m+n^+ = (m+n)^+ = m^+ + n)$. *Es decir,* $m+(n+1) = (m + n) + 1 = (m + 1) + n$.

(*) Como $m + n^+ = S_m(n^+) = (S_m(n))^+ = (m + n)^+$,

bastará demostrar que $m^+ + n = (m + n)^+$; lo haremos por inducción sobre n:

(i) Si $n = 0$, entonces $m^+ + 0 = m^+ = (m + 0)^+$ siendo la propiedad modulativa la justificación de las dos igualdades.

(ii) Supongamos que $m^+ + n = (m + n)^+$.

$$m^+ + n^+ = S_{m^+}(n^+) = (S_{m^+}(n))^+ = (m^+ + n)^+$$

y usando la hipótesis de inducción se tiene que la última expresión es $((m+n)^+)^+$ y por (*), esta última expresión es $(m+n^+)^+$, o sea que $m^+ + n^+ = (m + n^+)^+$, con lo cual la propiedad vale para n^+.

Propiedad Asociativa de la Adición.

$$(\forall k)(\forall m)(\forall n)((k + m) + n = k + (m + n)).$$

Se prueba por inducción sobre n:

(i) Si $n = 0$, $(k + m) + 0 = k + m = k + (m + 0)$ (por la propiedad modulativa).

(ii) Supongamos válida para n: $(k + m) + n = k + (m + n)$; entonces

$$\begin{array}{lll} (k + m) + n^+ = ((k + m) + n)^+ & & = (k + (m + n))^+ \\ \quad (1) & & (2) \\ = k + (m + n)^+ & & = k + (m + n^+) \\ (3) & & (4) \end{array}$$

Nota: (1), (3) y (4) son válidas por la parte (*) del lema anterior; (2) es simplemente la hipótesis de inducción.

Conmutatividad de la Adición.

$$(\forall m)(\forall n)(m + n = n + m).$$

Se prueba por inducción sobre m:

(i) Si $m = 0$, $0 + n = n = n + 0$ por ser 0 el módulo de la adición.

(ii) Supongamos que $m + n = n + m$.

$$m^+ + n = (m + n)^+ = (n + m)^+ = n + m^+$$

ya que las igualdades primera y tercera son válidas por el lema anterior y la segunda es la hipótesis de inducción.

Propiedad Cancelativa de la Adición.

$$(\forall m)(\forall n)(\forall k)((m + n = k + n) \longrightarrow m = k)$$

basta hacer inducción sobre n:

(i) Si $n = 0$, $(m + 0 = k + 0) \longrightarrow m = k$ por la propiedad modulativa.

(ii) Supongamos que vale para n y demostremos la propiedad para $n + 1$:

Si $m+(n+1) = k+(n+1)$, por la propiedad asociativa (o por la parte (*) del lema anterior) se tiene que $(m+n)+1 = (k+n)+1$ o sea $(m+n)^+ = (k+n)^+$ y por el axioma quinto de Peano, $m + n = k + n$ y usando la hipótesis de inducción, $m = k$.

Monotonía de la Adición.

$$(\forall m, n, k \in \mathbb{N})(m < n \longleftrightarrow m + k < n + k)$$

En un sentido significa que se puede sumar a los dos miembros de una desigualdad un mismo número natural y la desigualdad se conserva; en el sentido recíproco equivale a cancelar un mismo sumando sin que la desigualdad se altere.

Demostración. Por inducción sobre k, usando el lema 1 y la proposición 12 de la sección 2. La dejamos al lector junto con otras que aparecen más adelante, para que de pasivo espectador pase a convertirse en actor. □

Definiremos ahora la multiplicación en términos de la adición, como nos la han enseñado desde la escuela primaria: $1m = m$, $2m = m + m$, $3m = m + m + m$, etc., es decir como una suma repetida de sumandos iguales. De manera rigurosa: si para cada m natural tomamos en el teorema de definición por recurrencia como f a la función $S_m : \mathbb{N} \to \mathbb{N}$ (usada para definir la adición) y elegimos $a = 0$ en $\mathbb{N}$, dicho teorema nos garantiza la existencia de una única función $P_m : \mathbb{N} \longrightarrow \mathbb{N}$ tal que

$$(\alpha) \quad P_m(0) = 0 \quad \text{y}$$
$$(\beta) \quad P_m(n^+) = S_m(P_m(n)) = m + P_m(n).$$

Hallemos los valores de P_m en algunos números naturales:

$$P_m(1) = P_m(0^+) = m + P_m(0) = m + 0 = m$$
$$P_m(2) = P_m(1^+) = m + P_m(1) = m + m$$
$$P_m(3) = P_m(2^+) = m + P_m(2) = m + (m + m)$$

Estas igualdades, de acuerdo con nuestro propósito previo, nos sugieren definir la multiplicación en la forma

$$nm = P_m(n)$$

Esta definición transforma las propiedades (α) y (β) en

$$(\alpha^*) \quad 0m = 0$$
$$(\beta^*) \quad n^+m = (n + 1)m = m + nm = nm + m \quad .$$

La última igualdad se debe a la conmutatividad de la adición.

Es ahora relativamente fácil demostrar por inducción las propiedades básicas de la multiplicación de naturales.

Propiedad Modulativa de la multiplicación.

$$(\forall m)(m \cdot 1 = m = 1 \cdot m)$$

Demostración. Como $1m = P_m(0^+) = m + P_m(0) = m + 0 = m$, basta establecer por inducción que $m1 = m$; en efecto:

(i) $0 \cdot 1 = 0$ por (α^*)

(ii) Supongamos que $m \cdot 1 = m$;

$$\begin{aligned}(m + 1) \cdot 1 &= m \cdot 1 + 1 \quad \text{por } (\beta^*) \\ &= m + 1 \quad \text{por hipótesis de inducción.}\end{aligned}$$

□

Distributividad de la multiplicación por la izquierda con respecto a la adición .

$$(\forall k, m, n \in \mathbb{N})(k(m + n) = km + kn) \quad .$$

Demostración. Por inducción sobre k:

$$\begin{aligned}0(m + n) &= 0 && (\text{por } \alpha^*) \\ &= 0 + 0 && (\text{por ser 0 el módulo de } +) \\ &= 0m + 0n && (\text{por } \alpha^*)\end{aligned}$$

Supongamos $k(m + n) = km + kn$.

$$\begin{aligned}(k + 1)(m + n) &= k(m + n) + (m + n) && (\text{por } \beta^*) \\ &= (km + kn) + (m + n) && (\text{Hipótesis de inducción}) \\ &= (km + m) + (kn + n) && (\text{conmut. y asociat. de } +) \\ &= (k + 1)m + (k + 1)n && (\text{por } \beta^*)\end{aligned}$$

□

LEMA 2. $(\forall m \in \mathbb{N})(m \cdot 0 = 0)$.

Demostración. Es trivial por inducción y la dejamos al lector □

Conmutatividad de la Multiplicación.

$$(\forall m, n \in \mathbb{N})(mn = nm)$$

Demostración. Debe hacerla por inducción sobre m el lector; en ella usará el lema 2 y la propiedad modulativa de la multiplicación. □

Como consecuencia se obtiene la distributividad de la multiplicación con respecto a la adición.

Asociatividad de la Multiplicación.

$$(\forall m, n, k \in \mathbb{N})((mn)k = m(nk))$$

Demostración. Por inducción sobre m y también debe hacerla el lector □

LEMA 3. $(\forall n, m \in \mathbb{N})(n \neq 0 \vee m \neq 0 \longrightarrow n + m \neq 0)$

Demostración. Si $n \neq 0$, existe k en $\mathbb{N}$ tal que $n = k^+$ (ejercicio 9 de la sección 2) y $n + m = k^+ + m = (k + m)^+$ (lema 1) y el resultado se sigue del axioma 4 de Peano. Igualmente se procede si $m \neq 0$. □

La proposición contrarrecíproca del lema 3 nos dice que 0 es el único natural con inverso aditivo en $\mathbb{N}$.

LEMA 4. $(\forall m, k \in \mathbb{N})(mk = 0 \wedge k \neq 0 \longrightarrow m = 0)$

Demostración. Por inducción sobre k.

(i) Para $k = 0$ el resultado se sigue trivialmente por ser en este caso falso el antecedente de la implicación; por si las dudas del lector, para $k = 1$, se tiene $m \cdot 1 = 0 \longrightarrow m = 0$ por ser 1 el módulo de la multiplicación.

(ii) $m(k + 1) = 0$ si y sólo si $mk + m = 0$, si y sólo si $mk = 0 \wedge k = 0$. De donde, en particular, $m = 0$.

La primera equivalencia es inmediata y la segunda se sigue por el lema 3. □

Propiedad Cancelativa de la Multiplicación.

$$(\forall m, n, k \in \mathbb{N})(mk = nk \wedge k \neq 0 \longrightarrow m = n)$$

Demostración. Por inducción sobre n.

(i) Si $n = 0$, $mk = 0k \wedge k \neq 0 \longrightarrow mk = 0 \wedge k \neq 0$, y por el lema 4 se concluye $m = 0$, o sea que $m = n$.

(ii) Supongamos válida la propiedad para n. Sea $mk = (n + 1)k$ con $k \neq 0$; si fuese $m = 0$, se tendría $0k = 0 = (n+1)k = nk + k$ y por la contrarrecíproca del lema 3, $nk = 0 = k$, siendo contradictorio con la hipótesis $k \neq 0$. De modo que $m \neq 0$ y existe entonces s en $\mathbb{N}$ tal que $m = s + 1$ (ejercicio 9, §2), con lo cual la hipótesis se transforma en

$$(s + 1)k = (n + 1)k \wedge k \neq 0 \quad ,$$

o sea

$$sk + k = nk + k \wedge k \neq 0$$

de donde, por la cancelativa de la adición,

$$sk = nk \wedge k \neq 0$$

y por la hipótesis de inducción, $s = n$, es decir $m = s + 1 = n + 1$, siendo también válida para $n + 1$, quedando demostrado. □

Por último definiremos la *exponenciación* como multiplicación iterada de factores iguales. El teorema de definición por recurrencia aplicado a la función $P_m : \mathbb{N} \longrightarrow \mathbb{N}$ una vez escogido $a = 1$, produce una única función $e_m : \mathbb{N} \longrightarrow \mathbb{N}$ tal que

$$e_m(0) = 1$$
$$e_m(n^+) = P_m(e_m(n)) = m \cdot e_m(n)$$

Hallemos algunos de sus valores:

$$\begin{aligned} e_m(0) &= 1 \\ e_m(1) &= e_m(0^+) = m \cdot e_m(0) = m \cdot 1 = m \\ e_m(2) &= e_m(1^+) = m \cdot e_m(1) = m \cdot m \\ e_m(3) &= e_m(2^+) = m \cdot e_m(2) = m \cdot (m \cdot m) \\ &\vdots \end{aligned}$$

En consecuencia, definimos m^n como $e_m(n)$; las dos propiedades anteriores, características de la potenciación, vienen a ser entonces

$$m^0 = 1$$
$$m^{n+1} = m \cdot m^n = m^n \cdot m.$$

Son sencillas y bastante conocidas las demostraciones (por inducción) de las propiedades de la exponenciación, por lo cual las dejamos como ejercicio:

(a) $1^n = 1$, cualquiera sea el natural n.

(b) $m^1 = m$, para todo m en $\mathbb{N}$.

(c) $(\forall m, n, k \in \mathbb{N})(k^m \cdot k^n = k^{m+n})$.

(d) $(\forall m, n, k \in \mathbb{N})((mn)^k = m^k \cdot n^k)$.

(e) $(\forall m, n, k \in \mathbb{N})((k^m)^n = k^{(mn)})$.

Creemos que con el trabajo realizado hemos establecido los resultados básicos para poder desarrollar a partir de ellos la mayor parte de la aritmética de los naturales. Terminamos la sección demostrando los hechos más comunes acerca de los conjuntos finitos.

PROPOSICIÓN 19. *Si E y F son conjuntos finitos disyuntos, su reunión también es finita y además $\#(E \cup F) = \#(E) + \#(F)$.*

Demostración. Si $F = \emptyset$, entonces $\#(F) = 0$ y el resultado se obtiene inmediatamente; supongamos que $\#(E) = m$ y $\#(F) = n > 0$; existen biyecciones $f : E \longrightarrow m$ y $g : F \longrightarrow n$; si $s_m : n \longrightarrow m + n$ dada por $s_m(x) = m + x$ es una restricción de S_m, se tiene que s_m es inyectiva a causa de la propiedad cancelativa de la adición, de modo que la función compuesta $F \xrightarrow{g} n \xrightarrow{s_m} m+n$ tal que $x \longrightarrow m+g(x)$, es también inyectiva; además su recorrido $s_m(g(F)) = \{m, m+1, \cdots, m+(n-1)\}$ es disyunto con $F(E) = m = \{0, 1, \cdots, m-1\}$, de manera que según el teorema 8 del capítulo III.

$$f \cup (s_m \circ g) : E \cup F \longrightarrow m \cup \{m, m+1, \cdots, m+(n-1)\} = m+n \quad ,$$

también es una función inyectiva y siendo evidentemente sobreyectiva, es una biyección de $E \cup F$ en $m + n$, luego

$$\#(E \cup F) = m + n = \#(E) + \#(F)$$

quedando demostrado. □

PROPOSICIÓN 20. *Si E y F son conjuntos finitos cualesquiera, también $E \cup F$ es finito y $\#(E \cup F) \leq \#(E) + \#(F)$.*

Demostración. Por el ejercicio 17 de la sección 3 del capítulo I se tiene que E y $F - E$ son disyuntos y $E \cup F = E \cup (F - E)$, siendo finito por la proposición anterior y además

$$\#(E \cup F) = \#(E \cup [F - E]) = \#(E) + \#(F - E) \leq \#(E) + \#(F).$$

□

Los resultados anteriores pueden generalizarse para cualquier número (natural) de conjuntos finitos:

PROPOSICIÓN 21.

a) *Si $A_1, A_2, \cdots, A_n$ con n en $\mathbb{N}^*$ son conjuntos finitos disyuntos dos a dos, entonces su unión es un conjunto finito y*

$$\#(A_1 \cup A_2 \cup \cdots \cup A_n) = \#(A_1) + \#(A_2) + \cdots + \#(A_n).$$

b) *La unión de una colección finita de conjuntos finitos también es un conjunto finito.*

La demostración de la parte a) se hace por inducción usando la proposición 19, y la de la parte b) se obtiene aplicando el ejercicio 9 de la sección 5 del capítulo I y la parte a) ya supuestamente probada; dejamos los detalles al lector.

PROPOSICIÓN 22. *El producto cartesiano de dos conjuntos finitos es también finito y su número de elementos es igual al producto de los cardinales de los factores.*

Demostración. Sean E y F conjuntos finitos; debemos probar que $E \times F$ también lo es y que $\#(E \times F) = \#(E) \cdot \#(F)$. Si uno de los dos conjuntos es vacío, también $E \times F$ es vacío y la igualdad anterior se cumple inmediatamente ya que $(\forall n \in \mathbb{N})(n \cdot 0 = 0)$. Supongamos entonces que $E \neq \emptyset \neq F = \{f_1, f_2, \cdots, f_n\}$.

$$E \times F = (E \times \{f_1\}) \cup (E \times \{f_2\}) \cup \cdots \cup (E \times \{f_n\})$$

Como $\#(E \times \{f_k\}) = \#(E)$, para todo $k = 1, 2, \cdots, n$, se tiene que $E \times F$ es finito; además los conjuntos que figuran en la unión anterior son disyuntos dos a dos

$$f_i \neq f_j \longrightarrow (E \times \{f_i\}) \cap (E \times \{f_j\}) = \emptyset$$

porque las parejas ordenadas del uno difieren por lo menos en la segunda componente de las parejas ordenadas del otro. La primera parte de la proposición 21 implica entonces que

$$\begin{aligned} \#(E \times F) &= \#(E \times \{f_1\}) + \#(E \times \{f_2\}) + \cdots + \#(E \times \{f_n\}) \\ &= \#(E) + \#(E) + \cdots + \#(E) \quad (n \text{ veces}) \\ &= n \cdot \#(E) = \#(E) \cdot n = \#(E) \cdot \#(F) \end{aligned}$$

□

PROPOSICIÓN 23. *Si E es finito, también $\mathcal{P}(E)$ lo es y además* $\#(\mathcal{P}(E)) = 2^{\#(E)}$.

Demostración. En realidad fue hecha por inducción anticipadamente al final de la sección 3 del capítulo I. □

Ejercicios

1. Haga todas las demostraciones dejadas como trabajo para el lector.

2. Use la monotonía de la adición y la transitividad del orden estricto para demostrar que

$$(m < n \wedge k < l) \longrightarrow (m + k < n + l).$$

3. Ayudándose del ejercicio anterior, demuestre por inducción sobre k la monotonía de la multiplicación

$$(m < n \wedge k > 0) \longrightarrow (mk < nk).$$

4. Dados dos naturales cualesquiera m y n, demuestre por inducción sobre n que

$$m \leq n \quad \text{si y sólo si existe } k \text{ en } \mathbb{N} \text{ tal que } \quad m + k = n.$$

Pruebe que dicho k es único. A este único k tal que $m + k = n$ se le llama *la diferencia entre n y m* y se le designa por $n - m$.

+5. Utilizando el teorema del binomio $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ y la propiedad de ser $\binom{n}{k}$, con $0 \leq k \leq n$, el número de subconjuntos con k elementos que posee un conjunto con n elementos, realice una nueva demostración de la proposición 23 anterior.

6. Demuestre por inducción que si $E_1, E_2, \cdots, E_n$, son conjuntos finitos, también su producto cartesiano es finito y que

$$\#(E_1 \times E_2 \times \cdots \times E_n) = \#(E_1) \cdot \#(E_2) \cdots \#(E_n).$$

7. Sean E y F conjuntos finitos con $E = \{a_1, a_2, \cdots, a_n\}$. Obsérvese que siendo una función f de E en F un conjunto de parejas ordenadas $\{(a_1, x_1), (a_2, x_2), \cdots, (a_n, x_n)\}$ con $x_1, x_2, \cdots, x_n$ en F, ella queda unívocamente determinada por la énupla (ordenada) de sus imágenes $(x_1, x_2, \cdots, x_n)$, sobreentendiéndose que $x_1 = f(a_1)$, $x_2 = f(a_2)$, $x_3 = f(a_3)$, $\ldots$, $x_n = f(a_n)$.
En consecuencia existen tantas funciones de E en F como énuplas $(x_1, x_2, \cdots, x_n)$ con $x_1, x_2, \cdots, x_n \in F$, es decir, como elementos tiene $F \times F \times \cdots \times F$ (n veces). Concluya, usando la finitud de $\mathcal{P}(E \times F)$ y el ejercicio anterior, que el conjunto de funciones de E en F es finito y que su número de elementos es $[\#(F)]^{\#(E)}$.

8. Para hacer ver que existen formas diferentes de trabajar, desarrollemos informalmente algo de aritmética cardinal. Supongamos que partiendo del vago concepto intuitivo de número de elementos de un conjunto ($\#(A)$), hemos llegado a las propiedades:

   (i) $A \approx \#(A)$

   (ii) $\#(A) = \#(B) \Leftrightarrow A \approx B$.

   Decimos que n *es un número cardinal* si existe un conjunto A tal que $n = \#(A)$.

   (a) Pruebe que dados los cardinales m, n existen conjuntos disyuntos A y B tales que $m = \#(A)$ y $n = \#(B)$.

   (b) Si m, n son cardinales tales que $m = \#(A)$ y $n = \#(B)$ y $A \cap B = \emptyset$, definimos $m + n$ como $\#(A \cup B)$. Demuestre que esta adición está bien definida (no depende de A ni de B), es asociativa, modulativa y conmutativa.

   (c) Análogamente, si m, n son cardinales tales que $m = \#(A)$ y $n = \#(B)$, definimos mn como $\#(A \times B)$. Pruebe que esta multiplicación está bien definida, es asociativa, modulativa y conmutativa.

   (d) Demuestre además que si n, m, p son cardinales,

$$m(n + p) = mn + mp.$$

   (e) Intente definir una relación de orden entre cardinales que cumpla con las propiedades de monotonía de la adición y de la multiplicación. ¿Habrá necesidad de imponer restricciones sobre los cardinales, o valdrán las propiedades de monotonía en general?

**

Capítulo 5

CONSTRUCCIÓN DE LOS SISTEMAS NUMÉRICOS

Continuando con las ideas expuestas en el capítulo anterior, construiremos los enteros y los racionales como ciertas colecciones de clases de equivalencia, clases obtenidas a partir de relaciones de equivalencia compatibles con las operaciones de adición y multiplicación pre-existentes, para que de esta forma las operaciones entre clases resulten ser un simple paso al cociente de las anteriores, en el sentido de los conceptos dados al final de la sección 5 del capítulo III.

5.1 LOS NÚMEROS ENTEROS

En el mundo actual, desde temprana edad se le crea a la persona la necesidad de disponer de números negativos: Temperaturas bajo cero, deudas, gol-diferencia en contra, y en la escuela la posibilidad de poder efectuar siempre la resta, ya que sólo cuando $m \geq n$ existe un natural k tal que $n + k = m$, no pudiéndose hallar, por ejemplo, un natural para colocar dentro del cuadrado

$$3 + \square = 2$$

de tal manera que la proposición resultante sea verdadera. Supongamos por ahora que conocemos los enteros; es fundamental observar que todos éstos se pueden obtener como diferencias entre naturales: $0 = 1 - 1$, $1 = 3 - 2$, $2 = 5 - 3$, $5 = 8 - 3$, $-1 = 1 - 2$, $-2 = 4 - 6$, $-8 = 25 - 33$, etc., o

sea que una pareja ordenada de números naturales determina un entero, a saber, la diferencia entre su primera y su segunda coordenadas. Una aproximación inicial hacia los enteros sería entonces el considerarlos como parejas ordenadas de naturales; $(1,1)$ representería al cero, $(3,2)$ al 1, $(1,2)$ al -1, $(4,6)$ al -2, etc.; en general (m,n) representaría al entero $m-n$.

Existe sin embargo un problema: se puede obtener la misma diferencia entre muchas parejas distintas; así $(8,4)$, $(4,0)$, $(6,2)$, y $(10,6)$ entre otras, poseen siempre como diferencia 4.

Debemos en consecuencia considerar como equivalentes a todas aquellas que produzcan la misma diferencia: $(8,4) \sim (4,0)$, $(2,5) \sim (3,6)$, $(5,5) \sim (1,1)$, etc. Pero como no podemos utilizar la resta para definir tal relación de equivalencia porque queremos es precisamente construir los enteros, soslayamos este obstáculo usando la suma:

$(8,4) \sim (6,2)$ o sea $8-4=6-2$ si y sólo si $8+2=6+4$ y

$(2,5) \sim (3,6)$ o sea $2-5=3-6$ si y sólo si $2+6=3+5$,

y de modo general, $(m,n) \sim (p,q) \Longleftrightarrow m+q=n+p$.

Conociendo ya lo que deseamos hacer, procedamos en forma oficial:

DEFINICIÓN 1. *Sea* $A = \mathbb{N} \times \mathbb{N}$. Definamos las siguientes operaciones en A:

$$(m,n) \oplus (p,q) = (m+p, n+q)$$
$$(m,n) \odot (p,q) = (mp+nq, mq+np).$$

La razón de tales definiciones radica en que según lo dicho, $(m,n) \oplus (p,q)$ representa $(m-n)+(p-q)$ o sea $(m+p)-(n+q)$ y análogamente $(m,n) \odot (p,q)$ sería $(m-n)(p-q) = (mp+nq)-(mq+np)$.

PROPOSICIÓN 1. *Las dos operaciones acabadas de definir son conmutativas en* A :

$$\begin{aligned}(m,n) \oplus (p,q) &= (m+p, n+q) = (p+m, q+n) \\ &= (p,q) \oplus (m,n).\end{aligned}$$

(La conmutatividad de $+$ en $\mathbb{N}$ hace válida la segunda igualdad).

$$\begin{aligned}(m,n) \odot (p,q) &= (mp+nq, mq+np) = (pm+qn, pn+qm) \\ &= (p,q) \odot (m,n),\end{aligned}$$

siendo verdadera la segunda igualdad por la conmutatividad de $+$ y $\cdot$ en $\mathbb{N}$.

Definimos ahora en A la relación siguiente:

$$(m,n) \approx (p,q) \quad \text{si y sólo si} \quad m+q=n+p.$$

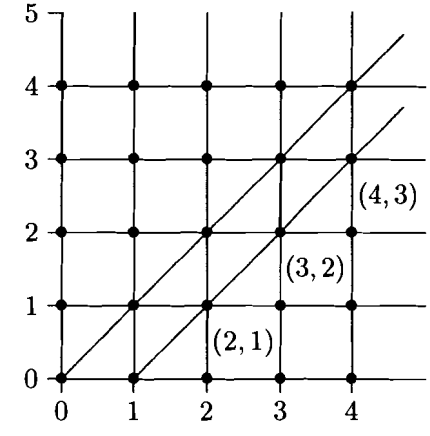
PROPOSICIÓN 2. *La relación acabada de definir es de equivalencia.*

Demostración. Por la conmutatividad de la adición en $\mathbb{N}$, $m+n=n+m$ lo cual significa $(m,n) \approx (m,n)$, cualquiera sea (m,n) en A (reflexividad).

Si $(m,n) \approx (p,q)$, entonces $m+q=n+p$ y por la simetría de la igualdad y la conmutatividad de la suma de naturales, $p+n=q+m$, o sea $(p,q) \approx (m,n)$.

Si $(m,n) \approx (p,q)$ y $(p,q) \approx (r,s)$ se tiene que $m+q=n+p$, y $p+s=q+r$ y sumando miembro a miembro: $m+q+p+s=n+p+q+r$ y cancelando $q+p$, $m+s=n+r$, es decir $(m,n) \approx (r,s)$, obteniéndose la transitividad. □

Las clases de equivalencia determinadas por esta relación pueden visualizarse al representar $\mathbb{N} \times \mathbb{N}$ gráficamente: Se hallan sobre rectas paralelas a



la diagonal.

TEOREMA 1. *La relación de equivalencia anterior es compatible con las operaciones* $\oplus$ *y* $\odot$ *definidas en* A.

Demostración. Según el ejercicio 10 de la sección 6 del capítulo III, al ser conmutativas las dos operaciones, basta probar que si $(m,n) \approx (p,q)$, entonces

$$(m,n) \oplus (r,s) \approx (p,q) \oplus (r,s) \quad \text{y}$$
$$(m,n) \odot (r,s) \approx (p,q) \odot (r,s),$$

siendo (m,n), (r,s) y (p,q) elementos cualesquiera de A.

En efecto: Si $(m,n) \approx (p,q)$, entonces $m+q = n+p$; sumando $r+s$ a los dos miembros, conmutando y asociando adecuadamente se obtiene

$$(m+r)+(q+s) = (n+s)+(p+r) \quad \text{o sea}$$
$$(m+r, n+s) \approx (p+r, q+s) \quad \text{esto es}$$
$$(m,n) \oplus (r,s) \approx (p,q) \oplus (r,s).$$

Análogamente, de $(m,n) \approx (p,q)$ se obtiene

$$(m+q = n+p) \wedge (n+p = m+q);$$

multiplicando por r y s respectivamente

$$(mr+qr = nr+pr) \wedge (ns+ps = ms+qs)$$

y sumando miembro a miembro:

$$mr+qr+ns+ps = nr+pr+ms+qs \quad \text{o sea}$$
$$[mr+ns]+[ps+qr] = [ms+nr]+[pr+qs] \quad \text{es decir}$$
$$(mr+ns, ms+nr) \approx (pr+qs, ps+qr) \quad \text{esto es}$$

$$(m,n) \odot (r,s) \approx (p,q) \odot (r,s),$$

quedando demostrado. □

El teorema acabado de demostrar significa que las dos operaciones $\oplus$ y $\odot$ se pueden pasar al conjunto cociente $A/\approx$, o sea que entre clases de equivalencia es correcto definir

$$[(m,n)] + [(r,s)] = [(m,n) \oplus (r,s)] \quad \text{y}$$
$$[(m,n)] \cdot [(r,s)] = [(m,n) \odot (r,s)] \quad .$$

El conjunto $A/\approx$ no es otro que el de los enteros y en adelante lo denotaremos por $\mathbb{Z}$.

TEOREMA 2. *Las operaciones $+$ y $\cdot$ (entre clases) definidas en $\mathbb{Z}$ gozan de las siguientes propiedades:*

(a) *Las dos son asociativas y conmutativas.*

(b) $[(m,m)]$ *es el módulo de* "$+$" (cualquiera sea $m \in \mathbb{N}$).

(c) $[(1,0)]$ *es el módulo de* la multiplicación.

(d) $[(n,m)]$ *es el inverso aditivo de* $[(m,n)]$.

(e) $\cdot$ *es distributiva con respecto a* $+$.

Demostración. La comprobación de (a), (c) y (e) es solo cuestión de rutina y la dejamos al lector.

Observemos que $(m,m) \approx (0,0)$ cualquiera sea m, luego $[(m,m)] = [(0,0)]$ y se tiene

$$[(p,q)] + [(0,0)] = [(p,q) \oplus (0,0)] = [(p,q)]$$

así que $[(m,m)]$ (ó $[(0,0)]$) es módulo de $+$.

Finalmente, $[(m,n)] + [(n,m)] = [(m,n) \oplus (n,m)] = [(m+n, n+m)] = [(m+n, m+n)] = [(0,0)]$, con lo cual se prueba (d). □

Entre las cosas que nos restan por establecer, es importante convencernos que los enteros que hemos construido realmente son aquellos que ya conocíamos.

PROPOSICIÓN 3. *Dado un entero $[(p,q)]$, existe un único natural n tal que ó $[(p,q)] = [(n,0)]$ ó bien $[(p,q)] = [(0,n)]$.*

Demostración. Dado $[(p,q)]$, según la ley de tricotomía del orden entre naturales, se cumple una única de las relaciones

$$p = q, \quad p > q, \quad p < q$$

En el primer caso $[(p,q)] = [(p,p)] = [(0,0)]$ y $n = 0$.

En el segundo caso, existe un único n tal que $p = n+q$ (ejercicio 4 de la sección 4 del capítulo anterior) y se tiene

$$[(p,q)] = [(n+q,q)] = [(n,0)]$$

ya que

$$(n+q,q) \approx (n,0).$$

Finalmente, cuando $p < q$ existe n no nulo único tal que $p+n = q$ y $[(p,q)] = [(p,p+n)] = [(0,n)]$. □

Si notamos por $\widehat{\mathbb{N}}$ al conjunto de los enteros de la forma $[(n,0)]$, es decir si $\widehat{\mathbb{N}} = \{[(n,0)] \mid n \in \mathbb{N}\}$, observamos que estos enteros son cerrados para la adición y multiplicación, operaciones con respecto a las cuales se comportan como si fueran los mismos números naturales:

$$[(m,0)] + [(n,0)] = [(m,0) \oplus (n,0)] = [(m+n,0)].$$
$$[(m,0)] \cdot [(n,0)] = [(m,0) \odot (n,0)] = [(mn+0, m0+0n)] = [(mn,0)].$$

Para sumarlos o multiplicarlos basta entonces sumar o multiplicar los naturales que aparecen en las primeras coordenadas y luego colocar ceros en las segundas y agregar los respectivos paréntesis. Otra forma más sofisticada de decir esto mismo es la siguiente: Si definimos la función $j : \mathbb{N} \longrightarrow \mathbb{Z}$ mediante $j(n) = [(n, 0)]$, es evidente que ésta es una inyección de $\mathbb{N}$ en $\mathbb{Z}$, la cual establece a su vez una biyección entre $\mathbb{N}$ y $\widehat{\mathbb{N}}$; además la forma como se suma y se multiplica en $\widehat{\mathbb{N}}$ significa que

$$j(m) + j(n) = j(m + n)$$

y

$$j(m) \cdot j(n) = j(m \cdot n),$$

razón por la cual se acostumbra decir que j es un isomorfismo de $\mathbb{N}$ en $\widehat{\mathbb{N}}$.

De todo lo anterior se concluye que para nuestro trabajo (i.e desde un punto de vista algebraico) no existe entre $\mathbb{N}$ y $\widehat{\mathbb{N}}$ otra diferencia que la notación para designar a sus elementos; es por tal razón que se acostumbra identificarlos; en adelante los consideraremos como iguales; diremos que $\mathbb{N}$ (en vez de $\widehat{\mathbb{N}}$) es un subconjunto de $\mathbb{Z}$ y en lugar de $[(m, 0)]$ escribiremos simplemente m Como

$$[(0, m)] + m = [(0, m)] + [(m, 0)] = [(m, m)] = [(0, 0)] = 0,$$

se tiene que $[(0, m)]$ es el inverso aditivo de m, es decir, $[(0, m)] = -m$; la notación queda entonces perfectamente simplificada y $\mathbb{Z}$ reducido a su forma usual:

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

Siendo la adición en $\mathbb{Z}$ conmutativa e invertiva, se puede definir su operación inversa, la diferencia, en todo $\mathbb{Z}$: para m y n cualesquiera en $\mathbb{Z}$,

$$m - n = m + (-n) = (-n) + m.$$

La diferencia, de ley de composición tan solo parcialmente definida en $\mathbb{N}$, pasa a ser totalmente definida en el conjunto de los enteros.

Se puede comenzar a demostrar en este momento toda una cadena de propiedades algebraicas de $\mathbb{Z}$; solamente enunciaremos algunas de ellas y dejaremos sus demostraciones como ejercicio de provecho para el lector, quien de hecho está familiarizado desde la escuela primaria, con muchas de las propiedades de los enteros.

Nota: En lo que sigue, denotaremos por $\mathbb{Z}^*$ al conjunto $\mathbb{Z} - \{0\}$ y por $\mathbb{N}^*$ al conjunto $\mathbb{N} - \{0\}$.

PROPOSICIÓN 4.

(a) $(\forall m \in \mathbb{Z})(-(-m) = m)$.

(b) $(\forall m \in \mathbb{Z}^* = \mathbb{Z} - \{0\})(m \in \mathbb{N}^* \ \veebar \ -m \in \mathbb{N}^*)$.

(c) $(\forall m, n \in \mathbb{Z})(m(-n) = -(mn) = (-m)n)$.

(d) $(\forall m, n \in \mathbb{Z})((-m)(-n) = mn)$. (Leyes de los signos)

(e) $(\forall m \in \mathbb{Z})(m \cdot 0 = 0)$.

(f) $(\forall m \in \mathbb{Z}^*)(mn = mk \longrightarrow n = k)$.

Para terminar, digamos algo sobre el orden usual de $\mathbb{Z}$: definamos $m < n$ como $(m - n) \in \mathbb{N}^*$ y $m \leqslant n$ como $(m - n) \in \mathbb{N}$. Usando la proposición 4 es fácil probar los dos resultados siguientes:

PROPOSICIÓN 5. *La relación "$\leqslant$" acabada de definir es de orden total en $\mathbb{Z}$.*

PROPOSICIÓN 6.

(a) $(\forall m, n \in \mathbb{Z})(m < n \longleftrightarrow m + k < n + k)$.

(b) $(\forall m, n \in \mathbb{Z})(\forall k > 0)(m < n \longrightarrow mk < nk)$.

(c) $(\forall m, n \in \mathbb{Z})(\forall k < 0)(m < n \longrightarrow mk > nk)$

Nótese que si $m, n \in \mathbb{Z}$ y $m < n$, decir que $(n - m) \in \mathbb{N}^*$ equivale a que $n = m + k$ con $k > 0$ y según el ejercicio 4 de la sección 4 del capítulo IV, m es menor que n en el sentido de la ordenación previamente dada a los naturales, resultando ser el orden definido en $\mathbb{Z}$ una extensión del orden que ya existía en $\mathbb{N}$, reafirmándose la corrección de la construcción que hemos logrado de $\mathbb{Z}$.

Ejercicios

1. Realice todas las demostraciones que hemos dejado como trabajo para el lector.

2. ¿ Es la operación $\oplus$ modulativa en $\mathbb{N} \times \mathbb{N}$? ¿Lo es $\odot$? ¿Es $\ominus$ invertiva?

3. Consideremos en $\mathbb{N} \times \mathbb{N}$ la relación

$$(m,n) \leq (p,q) \longleftrightarrow m+q \leq n+p$$

Demuestre que es de orden en $\mathbb{N} \times \mathbb{N}$ y que si $(m,n) \leqslant (p,q)$, y $(u,v) \approx (m,n)$ y $(r,s) \approx (p,q)$, entonces $(u,v) \leqslant (r,s)$. Deduzca que la anterior relación de orden puede pasar al cociente $\mathbb{N} \times \mathbb{N}/\approx$ y que en él es un orden total y satisface las propiedades (a), (b) y (c) de la proposición 6.

4. Pruebe que $\forall x \in \mathbb{Z},\ x^2 > 0$.

5. Si $c \in \mathbb{N}^*$, demuestre directamente que

$$[(m,n)] \cdot [(c,o)] = [(p,q)] \cdot [(c,0)] \longrightarrow [(m,n)] = [(p,q)]$$

y que

$$[(m,n)] \cdot [(0,c)] = [(p,q)] \cdot [(0,c)] \longrightarrow [(m,n)] = [(p,q)].$$

6. Pruebe que en $\mathbb{Z}$ toda ecuación de la forma $a+x=b$ (con a,b en $\mathbb{Z}$), tiene solución, pero existen ecuaciones del tipo $ax+b=c$ (con $a,b,c \in \mathbb{Z},\ a \neq 0$) sin solución.

5.2 LOS NÚMEROS RACIONALES.

La construcción de los números racionales a partir de los enteros se realiza siguiendo enteramente el mismo esquema empleado para la obtención de $\mathbb{Z}$ a partir de $\mathbb{N}$, motivo por el cual dejamos la mayor parte del trabajo al lector.

Es muy conocido que un número racional se puede expresar en forma de quebrado, es decir mediante una pareja ordenada de enteros, el primero de los cuales es el numerador y el segundo (no nulo) el denominador. También se sabe que $(m/n) = (p/q)$ si y sólo si $mq = np$; es entonces natural construir los racionales a partir de parejas ordenadas de enteros, definiendo entre ellos la relación de equivalencia sugerida por la última observación.

Sea $B = \mathbb{Z} \times \mathbb{Z}^* = \{(m,n) \mid m,n \in \mathbb{Z} \wedge n \neq 0\}$

Definimos en B las dos operaciones:

$$(m,n) \uplus (p,q) = (mq+np, nq)$$
$$(m,n) \otimes (p,q) = (mp, nq)$$

Al lector le deberán parecer familiares si recuerda cómo se suman y se multiplican quebrados, teniendo presente que (m,n) representa m/n.

PROPOSICIÓN 7. *Las dos operaciones anteriores son conmutativas y asociativas.*

La demostración es cuestión de rutina y la dejamos al lector, quien seguramente en primaria o secundaria la ha visto.

Consideremos en B la relación

$$(m,n) \simeq (p,q) \quad \text{si y sólo si} \quad mq = np.$$

PROPOSICIÓN 8. *La relación $\simeq$ es de equivalencia en B.*

Demostración. $(m,n) \simeq (m,n)$ ya que $mn = nm$.

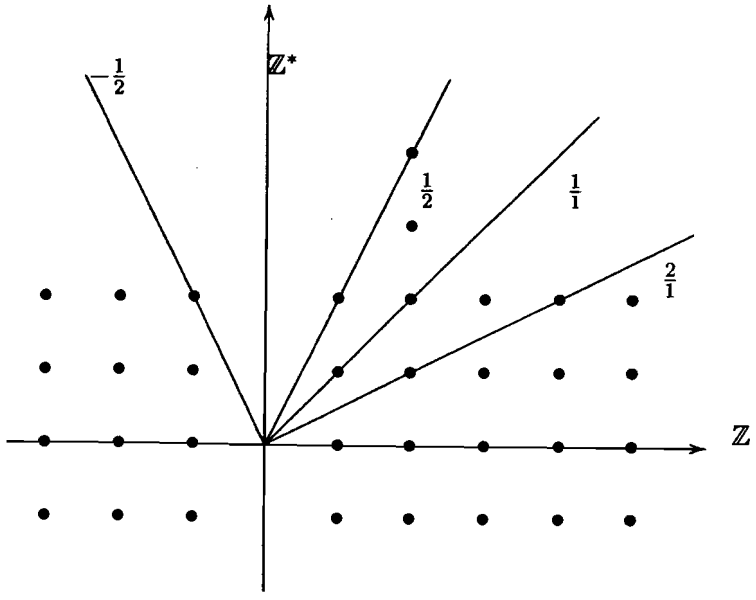
Si $(m,n) \simeq (p,q)$, $mq = np$ o sea $pn = qm$ y $(p,q) \simeq (m,n)$.

Si $(m,n) \simeq (p,q) \wedge (p,q) \simeq (r,s)$, entonces

$$(\alpha) \qquad mq = np \wedge ps = qr.$$

multiplicando miembro a miembro, $mqps = npqr$. Cuando $p \neq 0$, también $pq = qp \neq 0$ y este producto se puede cancelar, obteniéndose $ms = nr$, esto es $(m,n) \simeq (r,s)$. Cuando $p = 0$, (α) queda $mq = 0 \wedge qr = 0$ y siendo $q \neq 0$ $(q \in \mathbb{Z}^*)$ se sigue que $(m = 0) \wedge (r = 0)$ de modo que $ms = 0 = nr$ o sea $(m,n) \simeq (r,s)$. □

Las clases de equivalencia correspondientes pueden visualizarse al representar $\mathbb{Z} \times \mathbb{Z}^*$ gráficamente; se hallan sobre rectas que pasan por el origen.



TEOREMA 3. *La relación $\simeq$ es compatible tanto con $\otimes$ como con $\uplus$.*

Demostración.

a) Siendo $\uplus$ conmutativa, es suficiente probar que si $(m,n) \simeq (p,q)$ y (c,d) es cualquiera de B, entonces $(m,n) \uplus (c,d) \simeq (p,q) \uplus (c,d)$ o lo que es igual, que $(md+nc, nd) \simeq (pd+qc, qd)$ o equivalentemente $(md+nc)qd = nd(pd+qc)$, es decir que $mqd^2 + ncqd = npd^2 + ndqc$ Como $(m,n) \simeq (p,q)$, se tiene que $mq = np$; multiplicando la igualdad por d^2, $mqd^2 = npd^2$ y sumando $ncqd$ a los dos miembros se obtiene el resultado requerido.

b) Análogamente, si $(m,n) \simeq (p,q)$, $mq = np$ y multiplicando los dos miembros por cd, $mcqd = ndpc$ o sea $(mc, nd) \simeq (pc, qd)$, es decir

$$(m,n) \otimes (c,d) \simeq (p,q) \otimes (c,d).$$

□

DEFINICIÓN 2. *Notaremos* por $\mathbb{Q}$ al conjunto cociente $B/\simeq$ o sea a $(\mathbb{Z} \times \mathbb{Z}^*)/\simeq$.

A los elementos de este conjunto cociente los llamaremos *números racionales* y adoptaremos en vez de $[(m,n)]$ para tales clases de equivalencia, la notación $\frac{m}{n}$.

El teorema 3 significa que las operaciones $\uplus$ y $\otimes$ se pueden pasar al cociente, motivo por el cual son correctas las dos definiciones siguientes:

$$\frac{m}{n} + \frac{p}{q} = [(m,n) \uplus (p,q)] = \frac{mq+np}{nq}$$
$$\frac{m}{n} \cdot \frac{p}{q} = [(m,n) \otimes (p,q)] = \frac{mp}{nq}$$

Nótese además que $\frac{m}{n} = \frac{r}{s}$ si y sólo si $(m,n) \simeq (r,s)$, equivalente a $ms = nr$.

TEOREMA 4. *Las operaciones $+$ y $\cdot$ acabadas de definir en $\mathbb{Q}$, gozan de las siguientes propiedades:*

a) *Las dos son conmutativas y asociativas .*

b) *El módulo de $+$ es $\frac{0}{1}$ (o $\frac{0}{m}$ con $m \neq 0$ ya que $(0,m) \simeq (0,1)$).*

c) *$\frac{1}{1}$ (o $\frac{m}{m}$ con $m \neq 0$) es el módulo de la multiplicación.*

d) *El inverso aditivo de $\frac{m}{n}$ es $\frac{-m}{n}$ $\left(= \frac{m}{-n}\right)$.*

e) *Todo racional diferente del módulo de la adición posee inverso multiplicativo y $\left(\frac{m}{n}\right)^{-1} = \frac{n}{m}$.*

f) *La multiplicación es distributiva con respecto a la adición .*

Dejamos la demostración como ejercicio para el lector.

Es entonces posible definir en $\mathbb{Q}^* = \mathbb{Q} - \left\{\frac{0}{1}\right\}$ la división como operación inversa de la multiplicación:

$$\frac{m}{n} \div \frac{p}{q} = \frac{m}{n} \cdot \left(\frac{p}{q}\right)^{-1} = \frac{m}{n} \cdot \frac{q}{p} \quad \text{según e) del teorema 4.}$$

Al igual que en la construcción anterior, es necesario hacer notar que los racionales son una ampliación del sistema numérico de los enteros, es decir, que $\mathbb{Q}$ posee un subconjunto isomorfo con $\mathbb{Z}$. Basta llamar $\widehat{\mathbb{Z}}$ al conjunto de los racionales de la forma $\frac{m}{1}$; $\widehat{\mathbb{Z}} = \left\{\frac{m}{1} \mid m \in \mathbb{Z}\right\}$.

Este subconjunto es cerrado para la adición y la multiplicación en $\mathbb{Q}$:

$$\frac{m}{1}+\frac{n}{1}=\frac{m\cdot 1+1\cdot n}{1\cdot 1}=\frac{m+n}{1}$$

$$\frac{m}{1}\cdot\frac{n}{1}=\frac{m\cdot n}{1\cdot 1}=\frac{m\cdot n}{1}$$

Se observa que sumar o multiplicar en $\widehat{\mathbb{Z}}$ es lo mismo que hacerlo en $\mathbb{Z}$,trazar luego una raya horizontal y escribir 1 bajo ella; si definimos la función $i:\mathbb{Z}\longrightarrow\mathbb{Q}$ mediante $i(m)=\frac{m}{1}$, es inyectiva y establece una biyección entre $\mathbb{Z}$ y $\widehat{\mathbb{Z}}$; además

$$i(m)+i(n)=\frac{m}{1}+\frac{n}{1}=\frac{m+n}{1}=i(m+n)$$

y también

$$i(m)\cdot i(n)=i(m\cdot n),$$

resultando ser i un isomorfismo, o sea que en cuanto a nuestro trabajo concierne, no existe diferencia alguna entre $\widehat{\mathbb{Z}}$ y $\mathbb{Z}$, excepto la forma de notar sus elementos, razón por la cual en adelante siempre identificaremos $\frac{m}{1}$ con m y consideraremos a $\mathbb{Z}$ como un subconjunto de $\mathbb{Q}$.

Nos resta introducir la relación de orden usual entre racionales; una forma de hacerlo es la siguiente:

a) Dado un racional, siempre se puede escribir en forma tal que su denominador sea positivo. Por ejemplo, en vez de $\frac{4}{-3}$ y $\frac{-2}{-5}$ se toman $\frac{-4}{3}$ y $\frac{2}{5}$ respectivamente.

b) cuando vamos a comparar dos racionales con denominadores positivos, $\frac{m}{n}$ y $\frac{p}{q}$, podemos hacer común denominador "amplificando" cada quebrado por el denominador del otro, operación que no altera la relación existente por ser producto por un positivo (p.ej. para $\frac{2}{3}$ y $\frac{4}{5}$, se tendrá $\frac{2\times 5}{3\times 5}$ y $\frac{4\times 3}{5\times 3}$) de modo que la relación de orden la determinan los numeradores

$$2\times 5<4\times 3,\quad \text{luego}\quad \frac{2}{3}<\frac{4}{5}$$

La definición es entonces la siguiente: dados $\frac{m}{n}$ y $\frac{p}{q}$ racionales cualesquiera con denominadores positivos, $\frac{m}{n}<\frac{p}{q}$ significa $mq<np$, siendo esta última la relación de orden definida en $\mathbb{Z}$.

c) Como mq y np son enteros, según la ley de tricotomía válida para el orden entre enteros, se cumple una única de las relaciones $mq<np$, $mq=np$, $np<mq$, lo cual implica la validez de la tricotomía en $\mathbb{Q}$: $\frac{m}{n}<\frac{p}{q}$, $\veebar$ $\frac{m}{n}=\frac{p}{q}$, $\veebar$ $\frac{p}{q}<\frac{m}{n}$.

Es entonces suficiente probar la transitividad del orden estricto para que automáticamente "$\leq$" resulte ser un orden total.

Si $\left(\frac{m}{n}<\frac{p}{q}\right)\wedge\left(\frac{p}{q}<\frac{r}{s}\right)$ con $n,q,s>0$, se tiene que

$$(mq<np)\wedge(ps<qr);$$

multiplicando por $s>0$ los miembros de la primera desigualdad y por $n>0$ los de la segunda, obtenemos $(mqs<nps)\wedge(nsp<qrn)$ luego, por transitividad del orden en $\mathbb{Z}$, $mqs<qrn$ y cancelando $q>0$, $ms<rn$ o sea $\frac{m}{n}<\frac{r}{s}$.

d) La relación acabada de considerar es una extensión del orden existente en $\mathbb{Z}$, ya que $\frac{m}{1}<\frac{n}{1}$ si y sólo si $m\cdot 1<n\cdot 1$ si y sólo si $m<n$.

e) La relación de orden en $\mathbb{Q}$ satisface las propiedades de monotonía:

$$\text{Si}\quad \frac{m}{n}<\frac{p}{q}\quad\text{entonces}\quad \frac{m}{n}+\frac{r}{s}<\frac{p}{q}+\frac{r}{s}$$

y si $\frac{r}{s}>0$ y $\frac{m}{n}<\frac{p}{q}$, entonces $\frac{m}{n}\cdot\frac{r}{s}<\frac{p}{q}\cdot\frac{r}{s}$ y si $\frac{r}{s}<0$, la desigualdad se invierte.

f) Si $\mathbb{Q}^+=\left\{\frac{m}{n}\in\mathbb{Q}\;\middle|\;\frac{m}{n}>0\right\}$, se cumplen las siguientes propiedades:

(i) $\mathbb{Q}^+$ es cerrado para la adición y para la multiplicación.

(ii) $\forall x\in\mathbb{Q}^*=\mathbb{Q}-\{0\}$, se cumple que $(x\in\mathbb{Q}^+)\ \veebar\ (-x\in\mathbb{Q}^+)$.

Dejamos como ejercicio las demostraciones correspondientes a e) y f).

Ejercicios

1. Haga las pruebas dejadas como trabajo al lector.

2. Demuestre que los racionales cumplen con la propiedad arquimediana: $(\forall x \in \mathbb{Q})(\forall y \in \mathbb{Q}^+)(\exists n \in \mathbb{N})(x < ny)$.

3. El presente ejercicio tienen por objeto dar una forma alternativa de definir el orden en $\mathbb{Q}$.

   (a) Si definimos $\mathbb{Q}^+ = \left\{\frac{m}{n} \in \mathbb{Q} \mid mn \in \mathbb{Z}^+\right\}$, pruebe que $\mathbb{Q}^+$ es cerrado para la adición y para la multiplicación.

   (b) Demuestre que $\forall x \in \mathbb{Q}$, $x \neq 0$, se cumple una única de las relaciones $x \in \mathbb{Q}^+$ ó $-x \in \mathbb{Q}^+$.

   (c) Definimos $x \leq y$ como $((x - y = 0) \vee (x - y \in \mathbb{Q}^+))$. Pruebe que es una relación de orden en $\mathbb{Q}$.

   (d) Demuestre que la relación definida en c) satisface las propiedades de monotonía.

   (e) Pruebe que $1 \in \mathbb{Q}^+$.

4. Pruebe que para todo a en $\mathbb{Q}^*$, y todo $b \in \mathbb{Q}$, la ecuación $ax = b$ tiene una única solución en $\mathbb{Q}$.

5. Demuestre que si $x \in \mathbb{Q}^+$, entonces su inverso multiplicativo x^{-1} también pertenece a $\mathbb{Q}^+$.

6. Pruebe que entre dos racionales cualesquiera siempre existe otro racional.

5.3 LOS NÚMEROS REALES

¿Qué es un número real? Esta es una pregunta un tanto difícil de contestar, a la cual no se le dio respuesta satisfactoria sino hasta mediados del siglo XIX.

Al hombre le son suficientes los racionales para satisfacer la mayoría de sus necesidades numéricas; sin embargo, dentro de ellos no se encuentran soluciones para ecuaciones tan sencillas como $x^2 - 2 = 0$.

Los antiguos griegos creían que dos segmentos cualesquiera siempre eran *conmensurables*, es decir, que tomando uno de ellos como unidad para medir al otro, el resultado de la medición era un número racional. En esta creencia basaron buena parte de su trabajo sobre la semejanza de figuras y la teoría de proporciones. Hacia finales del siglo V a.c., los pitagóricos descubrieron que las diagonales de un cuadrado no son conmensurables con respecto al lado, o sea que $\sqrt{2}$ (el lado mide 1) no es un número racional.

De esta afimación hay una prueba en esencia realizada por los mismos griegos:

Supongamos que haya una fracción que valga $\sqrt{2}$; entonces también existe una fracción irreducible $\frac{p}{q}$ que es igual a $\sqrt{2}$, o sea que $\frac{p}{q} = \sqrt{2}$ con $\frac{p}{q}$ no simplificable, es decir con máximo común divisor de p y q igual a 1.

Pero

$$\frac{p}{q} = \sqrt{2} \Leftrightarrow \frac{p^2}{q^2} = 2 \Leftrightarrow p^2 = 2q^2$$

o sea que p^2 es par y en consecuencia p es par (ya que si $p = 2m + 1$, $p^2 = 2(2m^2 + 2m) + 1$ sería impar), luego $p = 2k$ y la última igualdad se transforma en $(2k)^2 = 2q^2$ o sea $4k^2 = 2q^2$ y simplificando por 2, $2k^2 = q^2$ luego q^2 es par y también q es par, $q = 2m$, así que $\frac{p}{q} = \frac{2k}{2m}$ sería simplificable por 2, contradiciendo la hipótesis de irreducibilidad.

Los griegos tuvieron entonces que revisar la casi totalidad de la teoría de las proporciones que habían desarrollado, buscando métodos que permitieran efectuar las demostraciones aun en casos no conmensurables.

Eudoxio propuso la siguiente definición de proporcionalidad: Si AB, CD, EF y GH son longitudes de segmentos, $AB : CD = EF : GH$ significa que para todo par de enteros positivos p, q

$$p \cdot CD < q \cdot AB \Leftrightarrow p \cdot GH < q \cdot EF$$

Es sumamente ingeniosa, eliminando la definición de número real (es decir, no definiendo lo que es una razón) y dando sólo el concepto de igualdad entre razones mediante el uso de naturales no nulos.

Modificando ligeramente lo anterior se obtiene

$$\frac{AB}{CD} = \frac{EF}{GH}$$

si y sólo si

$$(\forall p, q \in \mathbb{N}^*)(\frac{p}{q} < \frac{AB}{CD} \longleftrightarrow \frac{p}{q} < \frac{EF}{GH}).$$

Los números positivos (racionales o no) $\frac{AB}{CD}$ y $\frac{EF}{GH}$ son iguales si y sólo si todo racional menor que el uno es también menor que el otro; y recíprocamente.[1] Es una definición de igualdad entre reales muy astuta, útil y poderosa.

Cuando Richard Dedekind (1831-1916) estaba buscando un método para construir con todo el rigor posible los números reales, se encontró, para sorpresa de todos, con que el retomar las ideas de Eudoxio y darles un ropaje ligeramente diferente, era todo lo que se necesitaba. El trabajo de Dedekind (basado en el de Eudoxio) es esencialmente lo que vamos a presentar a continuación. Es la construcción de los reales más acorde con la teoría de conjuntos que hemos desarrollado y no necesita conocimientos sobre convergencia de sucesiones; presenta cada real como cierto conjunto de racionales, sin necesidad de pasar a clases de equivalencia.

Regresemos a la definición de igualdad entre números reales positivos dada por Eudoxio:

$$x = y \quad \text{si} \quad \text{sólo si} \quad (\forall p, q \in \mathbb{N}^*)(\frac{p}{q} < x \longleftrightarrow \frac{p}{q} < y).$$

para hacerla extensiva a todos los reales, basta tomar racionales cualesquiera:

$$x = y \quad \text{si} \quad \text{sólo si} \quad (\forall r \in \mathbb{Q})(r < x \longleftrightarrow r < y)$$

En otros términos:

$$x = y \quad \text{si} \quad \text{sólo si} \quad \{r \in \mathbb{Q} \mid r < y\} = \{r \in \mathbb{Q} \mid r < x\},$$

lo cual significa que *un número queda perfectamente determinado por el conjunto de todos los racionales que le preceden estrictamente.*

[1] Si no fuesen $\frac{AB}{CD}$ y $\frac{EF}{GH}$ iguales, existiría entre ellos un racional, el cual no cumpliría con la equivalencia de la definición

¿Por qué no tomar entonces como definición de número real al conjunto mismo de los racionales que le preceden estrictamente?

Eso fue precisamente lo que hizo Dedekind.

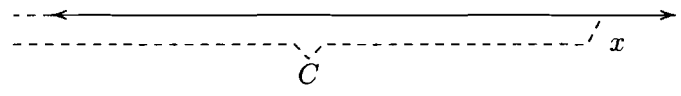
Analicemos un poco más la naturaleza de los conjuntos que definen números reales; sea $C = \{r \in \mathbb{Q} \mid r < x\}$.

(i) El conjunto C no es vacío, pues siempre existen racionales menores que cualquier real dado; tampoco C es todo $\mathbb{Q}$, ya que también existen racionales mayores que el real x.

(ii) Si $r \in C$ y s es un racional menor que r, entonces $s \in C$.

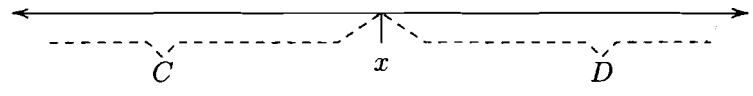
(iii) No existe un racional en C que sea el máximo de C ya que si r es cualquiera en C, por ser $r < x$ se puede hallar siempre un racional s entre r y x, o sea $r < s < x$, no siendo r el máximo.

Si pudiésemos dibujar este conjunto de racionales sobre una recta aparecería más o menos en la forma siguiente:



Nuestro dibujo no puede ser exacto porque sabemos que los puntos de una recta están en correspondencia biunívoca precisamente con el conjunto de los números reales y no con el de los racionales.

Al mirar el gráfico, no solamente vemos C (los menores que x) sino también el conjunto D de los mayores que x



Por este motivo, muchos autores prefieren decir que el número real x se define mediante una pareja (C, D) de conjuntos de racionales, y llaman a la pareja una *cortadura*. Sin embargo, siguiendo la ideas expuestas antes, continuaremos considerando como una cortadura al sólo conjunto C de la izquierda.

Una característica esencial de los números reales es su completez, la cual de modo burdo significa que si colocamos los reales sobre una recta (mediante la introducción en ésta de un sistema coordenado), los reales copan todos los puntos de la recta, de manera que si por algún procedimiento cortásemos la recta por cualquier punto, en dicho punto siempre se debería encontrar un número real. Todos los racionales que se hallan estrictamente a la izquierda del corte, vienen a constituir lo que hemos llamado una cortadura. El real se halla "pegado" a los racionales de la cortadura, o sea que entre él y los racionales de la cortadura no existe ningún otro real. En consecuencia, como lo decíamos antes, el real se halla determinado unívocamente por los racionales menores que él, es decir, por la cortadura; todo lo que haremos en la construcción que sigue es identificar al real con la cortadura que determina.

Procedamos formalmente:

DEFINICIÓN 3. *Una* cortadura *es un conjunto C de números racionales tal que* :

i) *C contiene al menos un racional, pero no contiene a todos los racionales.*

ii) *Si $r \in C$ y $s < r$ $(s \in \mathbb{Q})$, entonces $s \in C$.*

iii) *No existe en C un racional que sea el máximo de C.*

Nota: En adelante tomaremos como referencial al conjunto $\mathbb{Q}$. Así en vez de $s \in \mathbb{Q} - C$, escribiremos simplemente $s \notin C$.

PROPOSICIÓN 9. *Si $r \in C$ y $s \notin C$, entonces $r < s$.*

Demostración. Si se tuviera $s \leq r$, la propiedad ii) implicaría $s \in C$, contradictorio. □

Se pone de presente que todos los racionales que no están en C son cotas superiores de C, lo cual concuerda con nuestra idea intuitiva de que C está formado por *todos* los racionales menores que "algo". En especial:

TEOREMA 5. *Sea r un número racional cualquiera; el conjunto $C = \{s \in \mathbb{Q} | s < r\}$ es una cortadura. Además r es la mínima de las cotas superiores de C (r=Sup C).*

Demostración. Claramente C cumple i) y ii); la propiedad iii) se obtiene solamente con observar que si $s \in C$, $\frac{s+r}{2}$ también es un racional y que $s < \frac{s+r}{2} < r$, de modo que $\frac{s+r}{2} \in C$ y así ningún s de C es el máximo.

De otra parte $r \notin C$ (pues si lo estuviese se tendría la contradicción $r < r$) de modo que r es una cota superior de C (ver comentario a la proposición 9) y es la mínima, puesto que si $s \in \mathbb{Q}$ y $s < r$, entonces $s \in C$ y s ya no es cota superior de C porque en C no hay máximo elemento. □

A la cortadura acabada de construir la llamaremos una *cortadura racional* y la notaremos r_*.

Por comodidad introduciremos primero el orden entre cortaduras y luego sí las operaciones aritméticas.

DEFINICIÓN 4. *Sean C_1 y C_2 cortaduras; escribimos $C_1 < C_2$ si y sólo si existe un racional r tal que $r \in C_2$ y $r \notin C_1$.*

Aun cuando usamos el mismo símbolo para el orden usual de $\mathbb{Q}$ y el orden entre cortaduras, el contexto en que aparece aclara el sentido con el cual se está utilizando y evita las confusiones.

Si $C_1 < C_2$, al existir r en C_2 con $r \notin C_1$, necesariamente r es una cota superior de C_1, así que $\forall s \in C_1$, $s < r$ (la desigualdad es estricta porque $r \notin C_1$), y por la condición ii) de la definición 3, $s \in C_2$, o sea que $C_1 \subset C_2$, siendo estricta la contenencia debido a la existencia de un racional en C_2 que no está en C_1; se deduce que la relación de orden estricto entre cortaduras es simplemente la contenencia estricta entre conjuntos, de modo que "$\leq$" realmente es una relación de orden entre cortaduras. Como de costumbre, $C_1 \leq C_2$ significará $(C_1 < C_2) \underline{\vee} (C_1 = C_2)$ o sea $C_1 \subseteq C_2$. Si $0_* < C$, diremos que C es una cortadura positiva; análogamente C es negativa si $C < 0_*$, y C es no negativa si $0_* \leq C$.

TEOREMA 6. *El orden entre cortaduras satisface la tricotomía; en particular, es un orden total.*

Demostración. Sean C y E cortaduras; debemos probar que se cumple exactamente una de las relaciones $C = E$, $C < E$, $E < C$. Siendo ellas equivalentes a $C = E$, $C \subset E$, $E \subset C$, no es posible que se cumplan dos simutáneamente, así que basta demostrar que siempre se cumple al menos una de tales relaciones; supongamos que $C \neq E$; existe entonces en el conjunto C un elemento r que no está en E, caso en el cual $E < C$, o bien existe un racional s en E que no está en C, caso en el cual $C < E$. □

Pasamos ahora a definir la adición entre cortaduras; la idea central se halla en que si C yE son conjuntos de racionales menores que x y y respectivamente, las sumas $r + s$ con $r \in C$ y $s \in E$ serán menores que $x + y$, de manera que la colección de tales sumas deberá ser a su vez una cortadura.

PROPOSICIÓN 10. *Sean C_1 y C_2 cortaduras cualesquiera; entonces el conjunto $C = \{r + s \mid r \in C_1 \wedge s \in C_2\}$ es también una cortadura.*

Demostración. Se debe probar que C cumple las tres condiciones de la definición 3.

i) Como C_1 y C_2 no son vacíos, tampoco C lo es; sean u, v racionales tales que $u \notin C_1$ y $v \notin C_2$; de la proposición 9 se deduce

$$(\forall r \in C_1)(r < u) \wedge (\forall s \in C_2)(s < v),$$

luego por la monotonía de la adición en $\mathbb{Q}$, $r + s < u + v$, cualesquiera sean r en C_1 y s en C_2, así que $u + v \notin C$.

ii) Sean $r + s \in C$ y u un racional menor que $r + s$ (o sea $r \in C_1$, $s \in C_2$, $u < r + s$). Entonces $t = u - r < s$, es decir $u = r + t$ con t racional menor que s y aplicando ii) a C_2 se tiene que $t \in C_2$, de modo que $u = r + t \in C$.

iii) Sea $u \in C$; entonces $u = r + s$, con $r \in C_1$ y $s \in C_2$; como C_1 no tiene máximo, existe t en C_1 tal que $r < t$, luego $u = r + s < s + t$ y estando $t + s$ en C, u no es máximo de C.

□

DEFINICIÓN 5. *Si C_1 y C_2 son cortaduras, a la cortadura C de la proposición 10 la llamaremos la SUMA de C_1 y C_2 y la notaremos $C_1 + C_2$, es decir,*

$$C_1 + C_2 = \{r + s \mid r \in C_1 \wedge s \in C_2\}.$$

(Estamos usando el signo + para la adición entre racionales y para la adición entre cortaduras pero no creemos que se presenten confusiones por ello).

PROPOSICIÓN 11. *La adición entre cortaduras es asociativa y conmutativa.*

Demostración. La dejamos al lector ya que no es sino aplicar las correspondientes propiedades de la adición de racionales. □

PROPOSICIÓN 12. *La cortadura racional 0_* es el módulo de la adición de cortaduras.*

Demostración. Se debe probar que para cualquier cortadura C, los conjuntos $C + 0_*$ y C son iguales para lo cual es suficiente ver que cada uno es subconjunto del otro.

a) Sea $r \in C + 0_*$, con $r = s + t$, estando $s \in C$ y $t \in 0_*$, es decir con $t < 0$; al sumar s a los dos miembros de esta desigualdad se obtiene $r = s + t < s$ y por ii) se concluye que r pertenece a C.

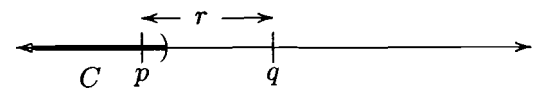
b) Sea $r \in C$; como C no tiene máximo, existe u en C tal que $r < u$, así que $r - u < 0$; se concluye que $r = u + (r - u)$ pertenece a $C + 0_*$.

□

La demostración de que toda cortadura tiene inversa aditiva, es un poco elaborada ya que si C es una cortadura, el conjunto $\{-r \mid r \in C\}$ no es una cortadura.

Necesitamos del siguiente lema:

LEMA 1. Sea C una cortadura y sea r un racional positivo. Entonces existen racionales p, q con $p \in C$, $q \notin C$, $q \neq Sup\, C$, y tales que $r = p - q$.



Como lo muestra la figura, intuitivamente significa que cualquier distancia racional $r > 0$ se puede dar entre un racional de C y otro que no pertenece a C.

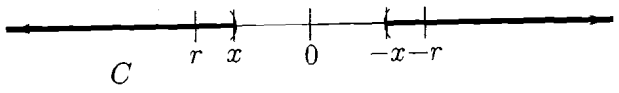
Demostración. Tomemos un racional cualquiera s en C y sumémosle múltiplos de r : s, $s+r$, $s+2r, \cdots$; llamemos s_n al racional $s+nr$, $n = 0, 1, 2, \cdots$ Siendo C acotada, existen naturales n tales que $s+nr \notin C$ (ya que $\mathbb{Q}$ cumple la propiedad arquimediana); como $s + 0 \in C$, tales naturales deberán ser mayores que cero, de modo que al mínimo de ellos (existe por ser $\mathbb{N}$ bien ordenado) le podemos notar por $m + 1$ con m en $\mathbb{N}$. Esto significa que

$$s_m \in C \quad \text{y} \quad s_{m+1} \notin C.$$

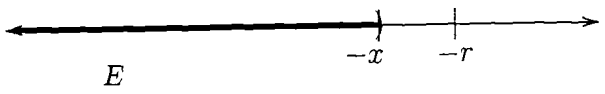
Si $s_{m+1} \neq Sup\, C$, el lema quedaría probado con solo tomar $q = s_{m+1}$ y $p = s_m$, puesto que $q - p = (s + (m+1)r) - (s + mr) = r$. Si $s_{m+1} = Sup\, C$, se tendría $s_m + \frac{r}{2} = s_{m+1} - \frac{r}{2} \in C$ y $s_{m+1} + \frac{r}{2} \notin C$, de modo que haciendo $q = s_{m+1} + \frac{r}{2}$ y $p = s_m + \frac{r}{2}$ también se obtiene $q - p = r$, quedando demostrado. □

PROPOSICIÓN 13. *Para toda cortadura C existe una cortadura E tal que $C + E = 0_*$.*

La búsqueda (informal) de la cortadura E puede hacerse de la siguiente manera: Si existiese $Sup\, C = x$, se tendría $C = \{r \in \mathbb{Q} \mid r < x\}$.



Siendo C algo así como una "cola a la izquierda", el gráfico sugiere que E debe estar constituida por todos los racionales menores que $-x$.



O sea que E estará formado por todos los racionales t menores que $-r$, para todo r en C, que sean distintos de $-x$. Pero

$$\{t \in \mathbb{Q} \mid (\forall r \in C)(t < -r)\} = \{t \in \mathbb{Q} \mid (\forall r \in C)(r < -t)\},$$

de modo que E será el conjunto de los t de $\mathbb{Q}$ tales que $-t$ sea cota superior de C, pero que no sea la mínima (puesto que $t \neq -x \longleftrightarrow -t \neq x$).

Demostraremos que efectivamente el conjunto E acabado de definir es una cortadura: La condición i) de la definición 3 se cumple ya que existen cotas superiores de C y no todo racional es cota superior de C. ii) Si $t \in E$ y s es un racional menor que t, entonces $-t < -s$ y siendo $-t$ una cota superior de C, también lo será $-s$ y además $-s$ no será la mínima, así que $s \in E$. iii) Sea t cualquiera en E; $-t$ es una cota superior de C y no es la mínima, de modo que al menos existe otra (notémosla $-s$) menor, $-s < -t$ y como $-s < \dfrac{-s+(-t)}{2} < -t$, también $\dfrac{-s-t}{2}$ es una cota superior de C y no es la mínima (ya que es mayor que $-s$), luego $\dfrac{s+t}{2} > t$, entonces t no es el máximo de E.

Nos resta comprobar que realmente $C + E = 0_*$.

a) Si $r \in C + E$, $r = s + t$ con $s \in C$ y $t \in E$, de manera que $-t$ es una cota superior de C (y no es la mínima), luego $s < -t$, de donde $s + t < 0$ o sea que $r \in 0_*$.

b) Sea $r \in 0_*$; $-r > 0$ y por el lema 1 existen racionales $p \in C$, $q \notin C$, $q \neq Sup\, C$ y $-r = q - p$ o sea $r = p + (-q) \in C + E$ ya que $-q \in E$ debido a que $-(-q) = q$ es cota superior de C (proposición 9) y no es la mínima.

La cortadura E inversa aditiva de C es única ya que si $\widehat{E}$ también lo fuese, se tendría

$$\widehat{E} = \widehat{E} + 0_* = \widehat{E} + (C + E) = (\widehat{E} + C) + E = 0_* + E = E.$$

En adelante la notaremos por $-C$.

Resumiendo:

TEOREMA 7. *El conjunto de todas las cortaduras posee estructura de grupo conmutativo con respecto a la adición* (dada en la definición 5).

PROPOSICIÓN 14. *La adición de cortaduras posee la propiedad de monotonía* (con respecto al orden dado en la definición 4).

Demostración. Sean C_1 y C_2 cortaduras tales que $C_1 < C_2$. Esto equivale a $C_1 \subset C_2$, de donde

$$\{r + s \mid r \in C_1 \wedge s \in C\} \subseteq \{r + s \mid r \in C_2 \wedge s \in C\}.$$

cualquiera sea la cortadura C, es decir $C_1 + C \leq C_2 + C$; la desigualdad debe ser estricta porque si $C_1 + C = C_2 + C$, al sumar $-C$ a los dos miembros se obtendría la contradicción $C_1 = C_2$. □

COROLARIO 1. *Si $C < 0_*$, entonces $-C > 0_*$.*

Demostración. Si fuese $-C \leq 0_*$, entonces $-C + C \leq 0_* + C$ y por consiguiente $0_* \leq C$. □

PROPOSICIÓN 15. *Dadas dos cortaduras cualesquiera C_1, C_2, siempre existe una única cortadura X tal que $C_1 + X = C_2$.*

A esta única X la notaremos por $C_2 - C_1$. Se concluye que la resta es una operación siempre definida entre cortaduras.

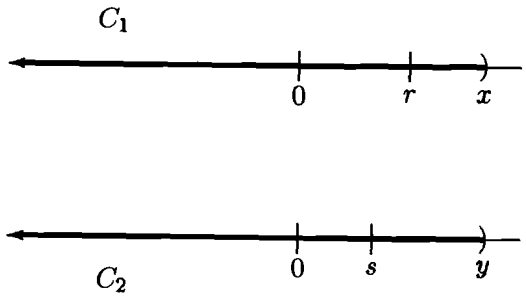
Demostración. La existencia se prueba tomando $X = C_2 + (-C_1)$ y la unicidad utilizando la cancelativa de la adición. □

A continuación vamos a introducir la multiplicación entre cortaduras, de cuyas propiedades dejaremos algunas demostraciones al lector para transformarlo de simple espectador en verdadero actor.

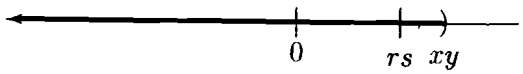
Si C_1 y C_2 son cortaduras, el conjunto $\{rs \mid r \in C_1 \wedge s \in C_2\}$ no es una cortadura; por ejemplo si C_1 y C_2 son cortaduras racionales negativas, el conjunto anterior es de números positivos, es una "cola a la derecha", la cual no es una cortadura.

¿Cómo definir entonces el producto? Hay necesidad de hacerlo por partes.

Primero consideremos el caso en que $C_1 \geq 0_*$ y $C_2 \geq 0_*$.



Si C_1 y C_2 fuesen cortaduras racionales $C_1 = x_*$ y $C_2 = y_*$, el producto $C_1 \cdot C_2$ debería ser $(xy)_*$, es decir tendría que ser el conjunto de todos los racionales menores que xy.



Dicho conjunto se puede obtener tomando el conjunto de los racionales negativos y uniéndole todos los productos rs que se pueden formar tomando $r \geq 0$, $s \geq 0$, $r \in C_1$ y $s \in C_2$.

Esto mismo puede hacerse para el caso general:

PROPOSICIÓN 16. *Sean C_1, C_2 cortaduras no negativas; el conjunto*

$$C = 0_* \cup \{rs \mid r \in C_1 \wedge r \geq 0 \wedge s \in C_2 \wedge s \geq 0\}$$

es una cortadura.

Demostración. Si $C_1 = 0_*$ ó $C_2 = 0_*$, claramente $C_1 \cdot C_2 = 0_*$ es una cortadura. Supongamos entonces que C_1 y C_2 son positivas.

i) Evidentemente C no es vacío y tampoco es todo $\mathbb{Q}$ ya que el producto de una cota superior de C_1 por otra de C_2 no está en C.

ii) Sean $u \in C$ y $v < u$, $v \in \mathbb{Q}$. Si $u < 0$, entonces $v \in 0_*$ y en consecuencia $v \in C$.

Si $u > 0$, existen $r \in C_1$, $s \in C_2$ con $r, s > 0$ tales que $u = rs$; sea $t = \dfrac{v}{r} < \dfrac{u}{r} = s$; $t \in C_2$ y así $v = rt \in C$.

iii) Como los elementos de 0_* no pueden ser máximos de C, sea $rs \in C$ con r en C_1 y $r, s \geq 0$; no existiendo máximos en C_1 ni en C_2, existirán p en C_1, q en C_2, $p > r$ y $q > s$; entonces $pq > rs \geq 0$ y estando pq en C, C no tendrá máximo.

□

DEFINICIÓN 6. *Si $C_1 \geq 0_*$ y $C_2 \geq 0_*$, la cortadura construida en la proposición 16 se llama el producto de las cortaduras C_1 y C_2, es decir,*

$$C_1 \cdot C_2 = 0_* \cup \{rs \mid r \in C_1 \wedge s \in C_2 \wedge r \geq 0 \wedge s \geq 0\}.$$

Nota. De la misma definición $C_1 \geq 0_* \wedge C_2 \geq 0_* \longrightarrow C_1 \cdot C_2 \geq 0_*$.

DEFINICIÓN 7. *Con toda cortadura C asociamos una cortadura $|C|$, llamada el valor absoluto de C, en la forma siguiente:*

Evidentemente $|C| \geq 0_*$ (ver corolario de la proposición 14) y $|C| = 0$ si y sólo si $C = 0_*$.

La definición de multiplicación se da entonces usando la de los valores absolutos y teniendo en cuenta las leyes de los signos.

DEFINICIÓN 8. *Sean C, E cortaduras cualesquiera; definimos $C \cdot E$ como*

a) $C \cdot E$ *si* $C \geq 0_*$ y $E \geq 0_*$.

b) $-(|C| \cdot E)$ *si* $C < 0_*$ y $E \geq 0_*$.

c) $-(C \cdot |E|)$ *si* $C \geq 0_*$ y $E < 0_*$.

d) $(|C| \cdot |E|)$ *si* $C < 0_*$ y $E < 0_*$.

Nótese que los productos están bien definidos y que dentro del paréntesis siempre aparece la multiplicación previamente definida de cortaduras no negativas.

LEMA 2. *Cualquiera sea la cortadura C, $C \cdot 0_* = 0_*$.*

Demostración. Como es realmente sencillo ver que $0_* \cdot 0_* = 0_*$, supongamos $C > 0_*$; entonces

$$C \cdot 0_* = 0_* \cup \{rs \mid r \in C \wedge s \in 0_* \wedge r \geq 0 \wedge s \geq 0\}$$

Pero el segundo conjunto de la unión es vacío por ser falso $s \in 0_* \wedge s \geq 0$, luego $C \cdot 0_* = 0_* \cup \emptyset = 0_*$.

Si $C < 0_*$, $C \cdot 0_* = -(|C| \cdot 0_*) = -(0_*) = 0_*$. □

LEMA 3. Si $C > 0_*$ y $E > 0_*$, entonces $C \cdot E > 0_*$.

Demostración. Es trivial ya que de la definición 6 se deduce que $C \cdot E \supseteq 0_*$ y la contenencia es estricta debido a que $0 \notin 0_*$ y $0 \in C \cdot E$. □

LEMA 4. *El conjunto de las cortaduras positivas es cerrado tanto para la adición como para la multiplicación de cortaduras.*

Demostración. Es una consecuencia inmediata de la monotonía de la adición y del lema 3. □

LEMA 5. *Si $E > 0_*$ y $F > 0_*$, entonces*

$$E + F = 0_* \cup \{e + f \mid e \in E \wedge f \in F \wedge e \geq 0_* \wedge f \geq 0_*\} = 0_* \cup P.$$

Esto significa que la suma de cortaduras positivas se puede obtener de manera análoga a como se efectúa el producto de cortaduras positivas.

Demostración. Trivialmente $E + F \supseteq P$ y como $0_* \subset E$ y $0 \in F$, también $E + F \supseteq \{r + 0 | r \in 0_*\} = 0_*$, de manera que $E + F \supseteq 0_* \cup P$.

Recíprocamente, sea $r \in E + F$; si $r \leq 0$ entonces $r \in 0_* \cup \{0\} \subseteq 0_* \cup P$. Supóngase $r > 0$; $r = u + v > 0$ con u en E y v en F; si $u, v > 0$, se tendá $u + v$ en P evidentemente; si $u < 0$ y $v > 0$, sumando v a la primera desigualdad, $0 < u + v < v$ de modo que $u + v \in F$ (propiedad ii)) y como $0 \in E$ se tendrá $u + v = 0 + (u + v)$ con $0 \in E$, $(u + v) \in F$, $0 \geq 0$, $u + v \geq 0$, es decir, $u + v \in P$. Análogamente se procede si $u > 0$ y $v < 0$. □

TEOREMA 8. *Sean C, E, F cortaduras cualesquiera; se tiene que:*

a) $C \cdot E = E \cdot C$ (conmutatividad).

b) $(C \cdot E) \cdot F = C \cdot (E \cdot F)$ (asociatividad).

c) $C \cdot (E + F) = C \cdot E + C \cdot F$ (distributividad).

Demostración. Si cualquiera de las cortaduras es 0_*, las tres propiedades se obtienen inmediatamente del lema 2 y la propiedad modulativa de la adición de cortaduras.

Es suficiente demostrar el teorema para el caso en el cual las tres cortaduras son positivas, ya que de éste y lo dicho se deducen inmediatamente los casos en los cuales algunas son negativas por la forma en que se dio la definición 8.

Dejamos que el lector pruebe las dos primeras propiedades y haremos la demostración de la tercera por ser un poco más elaborada.

Como suponemos C, E, $F > 0_*$, por el lema 4 se tiene que $C \cdot E$, $C \cdot F$, $C \cdot E + C \cdot F$, $E + F$, $C \cdot (E + F)$ son todas cortaduras positivas, así que $C \cdot (E + F) \supset 0_*$ y $C \cdot E + C \cdot F \supset 0_*$, de manera que para probar la igualdad de los conjuntos $C \cdot (E + F)$ y $C \cdot E + C \cdot F$ basta probar que contienen los mismos racionales no negativos; para hacerlo podemos suponer que siempre (tanto en $E + F$ como en $C \cdot E + C \cdot F$) se está trabajando con racionales positivos a causa del lema 5.

En efecto:

a) Si $u \in C \cdot (E + F)$, $u \geq 0$, entonces $u = rs$ con $r \geq 0$, $s \geq 0$, $r \in C$, $s \in E + F$. Según el lema 5, existen racionales no negativos e en E y f en F tales que $s = e + f$, luego $u = r(e + f) = re + rf$ y siendo $re \geq 0$ y $rf \geq 0$, u estará en $C \cdot E + C \cdot E$

b) Recíprocamente, si $u \in C \cdot E + C \cdot F$, $u \geq 0$, por el lema 5 existirán racionales no negativos p en $C \cdot E$ y q en $C \cdot F$ tales que $u = p + q$. Pero $p = r \cdot e$ y $q = s \cdot f$ con r, e, s, f no negativos y $r, s \in C$, $e \in E$, $f \in F$. Así $u = re + sf$.

Si $r = s$, $u = r(s + f)$ es un no negativo de $C \cdot (E + F)$. Si $r \neq s$, supongamos por ejemplo $r < s$; siendo $s > 0$, existe el cociente $\frac{r}{s}$ y es menor que 1, luego $\frac{r}{s} \cdot e < e$ y $\frac{r}{s} \cdot e$ estará en E y en consecuencia $u = s(\frac{r}{s} \cdot e + f)$ pertenece a $C \cdot (E + F)$, quedando demostrado. □

COROLARIO 2. *Si C y E son cortaduras cualesquiera*

$$(-C)E = -(CE)$$
$$(-C)(-E) = CE$$

Demostración. La dejamos como ejercicio para el lector; para lograrla es más fácil hacer uso de las propiedades ya establecidas (en especial de la distributividad) que trabajar directamente con cortaduras. □

PROPOSICIÓN 17. *$C \cdot E = 0_*$ si y sólo si $C = 0_* \vee E = 0_*$.*

Demostración. Del lema 2 se sigue que $C = 0_*$ o $E = 0_*$ implica que $C \cdot E = 0_*$. Recíprocamente, supongamos $CE = 0_*$; veamos que si $C \neq 0_*$, entonces $E = 0_*$. Sea $C > 0_*$; si $E > 0_*$, por el lema 3 $CE > 0_*$ (contradicción).

Si $E < 0_*$, por el Corolario 1 de la proposición 14 se tendría $-E > 0_*$, luego $C(-E) > 0_*$ y por el Corolario 1 del teorema 8, $-(CE) > 0_*$, o sea $CE < 0_*$, lo cual es contradictorio también, de manera que se deberá tener $E = 0_*$.

Análogamente se procede con $C < 0_*$. □

PROPOSICIÓN 18. *La multiplicación de cortaduras es modulativa con* 1_* *como módulo.*

Demostración. Dejamos al lector que pruebe $C \cdot 1_* = C$ cuando $C > 0_*$. Cuando $C = 0_*$ el lema 2 establece el resultado; si $C < 0_*$, $C = -|C|$ y $C \cdot 1_* = -(|C| \cdot 1_*) = -(|C|) = C$. □

PROPOSICIÓN 19. *Si* $E < F$ *y* $0_* < C$, *entonces* $C \cdot E < C \cdot F$.

Demostración. La dejamos al lector pero le ayudamos: Se debe tener en cuenta que $E < F \longleftrightarrow 0_* < F - E$ y usar el lema 4 junto con la distributividad y su corolario. □

TEOREMA 9. *Si* $C \neq 0_*$, *entonces existe una única cortadura* E *tal que* $C \cdot E = 1_*$.

Se acostumbra designar a esta única E por C^{-1} o por $\frac{1}{C}$.

Demostración. Es suficiente demostrar el teorema cuando $C > 0_*$ puesto que si $C < 0_*$, la definición 8 implica que $C^{-1} = -(|C|^{-1})$.

Supongamos en adelante $C > 0_*$; a semejanza del caso del inverso aditivo, definimos

$$E = 0_* \cup \{0\} \cup \{t \in \mathbb{Q} \mid t > 0 \wedge (\forall r \in C)(r < \frac{1}{t})\},$$

es decir, E es el conjunto de los racionales no positivos unido con aquellos t positivos tales que t^{-1} es cota superior de C. Se pide al lector que trabaje un poco (el autor ya lo ha hecho bastante) y pruebe que a) E es una cortadura y b) $C \cdot E = 1_*$.

La demostración de la unicidad del inverso multiplicativo es idéntica a la realizada para el inverso aditivo. □

Con el desarrollo que hemos efectuado se ha puesto de presente que el conjunto de las cortaduras con la adición, la multiplicación y el orden definidos, posee estructura de campo ordenado. Vamos a demostrar que las cortaduras poseen un subconjunto isomorfo con el también campo ordenado de los racionales, con lo cual el conjunto de las cortaduras se convierte en un excelente candidato para constituirse en el campo de los *números reales.*

LEMA 6. *Si* $p \in \mathbb{Q}$, *entonces* $-(p_*) = (-p)_*$.

Demostración. $-(p_*) = \{t \in \mathbb{Q} | -t$ es cota superior de p_* y $-t \neq Sup\, p_*\}$

$= \{t \in \mathbb{Q} | -t \geq p \wedge -t \neq p = Sup\, p_*\}$

$= \{t \in \mathbb{Q} | -t > p\}$

$= \{t \in \mathbb{Q} | t < (-p)\} = (-p)_*$.

□

COROLARIO 3. $|p_*| = |p|_*$

Demostración. Si $p \geq 0_*$, entonces $p_* \geq 0_*$ trivialmente de modo que $|p_*| = p_* = |p|_*$.

Si $p < 0$, $|p_*| = -(p_*) = (-p)_* = |p|_*$. □

PROPOSICIÓN 20. *El conjunto de las cortaduras racionales posee las propiedades siguientes:*

a) $p_* + q_* = (p + q)_*$.

b) $p_* \cdot q_* = (p \cdot q)_*$.

(Las operaciones de la izquierda son entre cortaduras y las de la derecha entre números racionales).

c) $p_* < q_*$ *si y sólo si* $p < q$.

Demostración.

a) Si $r \in p_* + q_*$, entonces $r = s + t$ con $s \in p_*$ y $t \in q_*$, es decir, con $s < p$ y $t < q$ luego $s + t < p + q$ y en consecuencia $r = s + t \in (p + q)_*$. Sea ahora $r \in (p + q)_*$; $r < p + q$; sea $h = p + q - r$; h es un racional positivo de modo que $s = p - \frac{h}{2} < p$ y $t = q - \frac{h}{2} < q$, luego $s \in p_*$ y $t \in q_*$ y $r = s + t \in p_* + q_*$.

b) Supongamos que $p > 0$ y $q > 0$; en este caso $p_* > 0_*$, $q_* > 0_*$, $pq > 0$ y $p_* q_* > 0_*$, de modo que según lo dicho en la demostración del teorema 8, basta considerar los elementos positivos. Si $r \in p_* \cdot q_*$ y $(r > 0)$, $r = st$ con $s > 0$, $t > 0$ y $s < p$, $t < q$, luego $st < pq$ y $r = st \in (pq)_*$. Recíprocamente si $r > 0$ y $r \in (pq)_*$, entonces $r < pq$ o sea $pq - r > 0$ y en consecuencia $\frac{pq - r}{p + q} > 0$ y según el ejercicio 6 de la sección 2, existe algún racional ε tal que $\frac{pq - r}{p + q} > \varepsilon > 0$; de donde

$$(p - \varepsilon)(q - \varepsilon) = pq - \varepsilon(p + q) + \varepsilon^2 > pq - \varepsilon(p + q) > r.$$

Como $(p-\varepsilon)(q-\varepsilon) \in p_*q_*$, también $r \in p_*q_*$.

Si $p = 0 \vee q = 0$, el lema 2 implica $p_*q_* = (pq)_*$. Si $p < 0 \wedge q > 0$,

$$p_*q_* = -(|p_*|q_*) = -(|p|q)_* = (-(|p|q))_* = (-|p| \cdot q)_* = (pq)_*,$$

en donde la primera igualdad se cumple por la definición del producto de cortaduras, la segunda por el corolario del lema 6, la tercera por haberse demostrado para racionales positivos, la cuarta por el lema 6 y las dos últimas trivialmente.

Análogamente se prueba en los demás casos.

c) Aun cuando se puede probar en forma directa, lo vamos ha hacer usando las propiedades vistas.

Cuando $r \in \mathbb{Q}$ y $r > 0$, trivialmente $r_* \supset 0_*$ o sea $r_* > 0_*$. pero $p < q \leftrightarrow q - p > 0$ implica $(q+(-p))_* > 0_*$ y por a), esta última desigualdad equivale a $q_* + (-p)_* > 0_*$ y por el lema 6 ésta es equivalente a $q_* + [-(p_*)] > 0_* \leftrightarrow q_* > p_*$ por la monotonía de la adición.

□

TEOREMA 10. *Las cortaduras racionales constituyen un campo ordenado isomorfo a* $\mathbb{Q}$.

Demostración. Es un corolario inmediato de la proposición anterior. □

TEOREMA 11. *Entre dos cortaduras cualesquiera siempre existe una cortadura racional.*

Demostración. Sean $C < E$ cortaduras cualesquiera; existe entonces (def. 4) un racional p en E que no está en C. No existiendo máximo en E, sea r un racional de E tal que $r > p$.

Como $r \notin r_*$ y $r \in E$, entonces $r_* < E$.

Puesto que $p < r$, $p \in r_*$ y no estando p en C, se sigue $C < r_*$ quedando demostrado el teorema. □

TEOREMA 12. *Sea C una cortadura cualquiera; entonces se verifica que $r \in C$ si y sólo si $r_* < C$.*

En otras palabras, $C = \{r \in \mathbb{Q} \mid r_* < C\}$.

Demostración. Sea $r \in C$; como $r \notin r_*$, entonces $r_* < C$. Recíprocamente, si $r_* < C$, existe un racional $s \in C$ tal que $s \notin r_*$ o sea $s > r$; como $s \in C$, la propiedad ii) de las cortaduras implica que $r \in C$. □

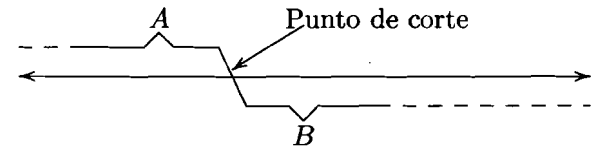
Como ya lo habíamos anunciado antes,

DEFINICIÓN 9. *En adelante a toda cortadura le llamaremos un número real.*

En consecuencia el campo ordenado de las cortaduras se denominará el campo ordenado de los números reales y de acuerdo con el teorema 10, a las cortaduras racionales las identificaremos con los números racionales y en lo que sigue las llamaremos simplemente números racionales. Al conjunto de los reales lo simbolizaremos por $\mathbb{R}$.

El Teorema 11 se traduce entonces como "entre dos reales cualquiera siempre existe un racional" y el teorema 12 viene a ser " Un número real es el conjunto de los racionales que le preceden".

Con esto hemos finalizado la construcción de $\mathbb{R}$; sin embargo, vamos a demostrar un par de resultados más, pertenecientes ya al análisis matemático, con el único objeto de hacer ver que el campo de los reales acabado de construir es el mismo que se supone conocíamos de antemano, para lo cual es suficiente probar el llamado axioma de completez, a saber, que "Todo subconjunto de $\mathbb{R}$ no vacío y acotado superiormente posee *Sup* en $\mathbb{R}$". Lo haremos a través de un interesante resultado el cual pone de presente que si con los números reales construyésemos cortaduras como lo hicimos con los racionales, nuevamente obtendríamos $\mathbb{R}$ (más exactamente, un campo ordenado isomorfo a $\mathbb{R}$); este mismo resultado hace ver que si colocamos los reales sobre una recta y por algún procedimiento la cortamos, el corte siempre se realiza por un número real, de modo que todo punto de la recta corresponde a algún real.



TEOREMA 13. *Sean A y B subconjuntos no vacíos y disyuntos de $\mathbb{R}$ tales que*

1. $A \cup B = \mathbb{R}$
2. *Todo elemento de A es estrictamente menor que todo elemento de B; entonces, existe un único real z tal que $x \leq z$ para todo x en A y $z \leq y$ para todo y en B.*

Demostración. Primero veamos lo concerniente a la existencia.

Sea C el conjunto de todos los racionales que pertenecen a las cortaduras de A, es decir, C es la reunión de las cortaduras (números reales) de A :

$$C = \{r \in \mathbb{Q} \mid (\exists E \in A)(r \in E)\}.$$

Veamos que C también es una cortadura.

i) No siendo A vacío, existen cortaduras E en A y como $E \subseteq C$, C no es vacío. Tampoco B es vacío y si $F \in B$ y $r \notin F$, entonces $(\forall E \in A)(r \notin E)$ puesto que $E < F$ (o sea $E \subset F$).

ii) Si $r \in C$ y $s < r$, como r pertenece a algún E de A y E es cortadura, $s \in E$ y en consecuencia $s \in C$.

iii) Análogamente, si $r \in C$, $r \in E$ para algún E de A, así que existe s en E tal que $r < s$, luego $s \in C$ y C no posee máximo.

Se concluye que C es un real y que $\forall E \in A$, $E \subseteq C$, es decir, $E \leq C$. probemos por contradicción que $C \leq F$ para todo F en B; si existiese algún F en B tal que $F < C$, existiría algún otro racional $r \in C$ y $r \notin F$, pero $r \in C$ implicaría $r \in E$ para algún E de A y esto significaría $F < E$, contrario a la parte ii) de la hipótesis.

Ahora demostraremos la unicidad: si existiesen dos reales C_1 y C_2 que cumplieran con las condiciones del teorema y por ejemplo $C_1 < C_2$, existiría un tercer real C_3 tal que $C_1 < C_3 < C_2$ (por el teorema 11). Pero $C_3 < C_2$ implicaría $C_3 \in A$, mientras que $C_1 < C_3$, implicaría $C_3 \in B$, contrario a la hipótesis $A \cap B = \emptyset$. □

COROLARIO 4. *Bajo las hipótesis del teorema 13, A contiene un máximo número real ó B contiene un mínimo.*

Demostración. Sea C la cortadura construida en la prueba del teorema 13; si $C \in A$, C es el máximo de A; si $C \in B$, C es el mínimo de B. □

Finalmente obtengamos la completitud de $\mathbb{R}$:

TEOREMA 14. *Todo subconjunto de $\mathbb{R}$ no vacío y acotado superiormente posee Sup en $\mathbb{R}$.*

Demostración. Sea X un subconjunto no vacío de reales acotado superiormente; definimos los dos conjuntos siguientes:

$$A = \{y \in \mathbb{R} \mid (\exists x \in X)(y < x)\} \quad \text{y} \quad B = \mathbb{R} - A.$$

Claramente ningún miembro de A es cota superior de X y todos los elementos de B son cotas superiores de X.

Mostraremos que A y B cumplen con las condiciones exigidas en la hipótesis del teorema 13: no siendo X vacío, tampoco lo es A; B no es vacío por ser X acotado superiormente; de la definición de A y B, éstos son disyuntos y además $A \cup B = \mathbb{R}$. si $y \in A$ y $u \in B$, entonces de una parte existe x en X tal que $x < y$ y de otra u es cota superior de X, luego $x < u$ y se concluye $y < x < u$ o sea $y < u$, siendo todo elemento de A menor que todo de B. Por el corolario del teorema 13, existe un número real z tal que z es el máximo de A o z es el mínimo de B, de manera que es suficiente probar que la primera alternativa no puede ocurrir: Si z estuviese en A, existiría x en X tal que $z < x$ y por el teorema 11 también existiría v real tal que $z < v < x$; entonces v estaría en A y z no sería máximo de A, quedando demostrado el teorema ya que la alternativa $z \in B$ significa que z es la mínima cota superior de X. □

Puede hacerse una demostración directa del axioma de completez de $\mathbb{R}$ (en vez de la anterior):

Sea A un conjunto no vacío de reales acotado superiormente; así A es un conjunto de cortaduras. Sea $\beta = \bigcup_{\alpha \in A} \alpha$. veamos que β *es una cortadura* (es decir, un real).

(i) $\beta \neq \mathbb{Q}$ porque A es acotado (existe $r \in \mathbb{Q}$, $r > \alpha$, $\forall \alpha \in A$, luego $r \notin \beta$).

(ii) $\beta \neq \emptyset$ obviamente.

(iii) Si $r \in \beta$ y $s < r$, $s \in \mathbb{Q}$, entonces existe $\alpha \in A$ tal que $r \in \alpha$ y como α es cortadura, $s \in \alpha$ y con mayor razón $s \in \beta$.

(iv) β no tiene máximo: si lo tuviese y fuese r, entonces $r \in \alpha$ para algún $\alpha \in A$ y α tendría máximo y no sería cortadura.

(v) β es el supremo de A ya que como $\alpha \subseteq \beta$ para todo $\alpha \in A$, entonces $\alpha \leq \beta$, para todo $\alpha \in A$. Si γ es otra cota superior de A, $\alpha \subseteq \gamma$ para todo $\alpha \in A$, luego $\bigcup_{\alpha \in A} \alpha \subseteq \gamma$ y por lo tanto $\beta \leq \gamma$.

Para el lector es conveniente saber que también existen otras formas de construír los números reales a partir de $\mathbb{Q}$, como lo son mediante "encajes de intervalos" de racionales y por medio de "sucesiones de Cauchy" de racionales. Si está interesado en ellas y desea compararlas con la construcción por cortaduras, puede consultar por ejemplo [11].

Ejercicios

1. Realice las demostraciones dejadas para ser efectuadas por el lector.

2. ¿Por qué la construcción dada para la cortadura inversa multiplicativa no produce una cortadura cuando el número es cero?

3. Usando el teorema 14, demuestre que en $\mathbb{R}$ sí posee solución la ecuación $x^2 - 2 = 0$.

4. Pruebe que todo subconjunto de $\mathbb{R}$ no vacío y acotado inferiormente posee Ínf en $\mathbb{R}$.

5. Demuestre que dado cualquier real, siempre existe un real estrictamente mayor y otro estrictamente menor.

6. Pruebe que $\mathbb{N}$ no es un subconjunto superiormente acotado de $\mathbb{R}$.

7. Demuestre que $\mathbb{R}$ satisface la propiedad arquimediana: dados x, y en $\mathbb{R}$ y $x > 0$, existe un natural n tal que $nx > y$.

8. Revise su concepto de sucesión (ver ejercicio 4, sección 3, cap IV); una sucesión como a, ar, ar^2, ar^3, $\cdots$, ar^n, $\cdots$ en la cual cada término se obtiene multiplicando al anterior por una constante r, se llama una progresión geométrica. Demuestre por inducción que

   (a) $S_n = a + ar + ar^2 + ar^3 + \cdots + ar^n = a\left(\dfrac{1 - r^{n+1}}{1 - r}\right)$.

   (b) Admitiendo que cuando $|r| < 1$ se tiene que $\lim_{n\longrightarrow\infty} r^n = 0$, pruebe que si $|r| < 1$, entonces
   $\dfrac{a}{1-r} = \lim_{n\longrightarrow\infty} S_n = a + ar + ar^2 + \cdots = \sum_{k=0}^{\infty} ar^k$.

9. (a) Usando el ejercicio anterior, demuestre que si el desarrollo decimal de un número real es periódico,
   $a = n \cdot b_1 b_2 \cdots b_k a_1 a_2 \cdots a_m a_1 a_2 \cdots a_m \cdots$,
   entonces a es un racional, hallando su valor p/q con p y q enteros.

   (b) Aplique el resultado obtenido para transformar en fraccionarios los reales siguientes:

   i. $0.999\cdots$
   ii. $0.12353535\cdots$
   iii. $0.002999\cdots$

   iv. $0.003000\cdots$
   v. $0.123454545\cdots$

10. Demuestre que todo decimal periódico no nulo con período cero, tiene también un desarrollo decimal (único) periódico con período nueve. (Ayuda: analice los ejercicios iii. y iv. anteriores).

11. Si en vez del sistema decimal usamos el binario, todo número real entre cero y uno se puede escribir en la forma

$$a_1 \cdot 2^{-1} + a_2 \cdot 2^{-2} + a_3 \cdot 2^{-3} + \cdots$$

la cual se acostumbra a escribir $0.a_1a_2a_3\cdots$, en donde para todo k, a_k es cero o uno.

   (a) Exprese en esta forma los reales 1/2, 1/4, 1/10, 1, 0.

   (b) Exprese como quebrado (en base 10) cada uno de los siguientes reales dados en el sistema binario:

   i. $0.1111\cdots$
   ii. $0.101111\cdots$
   iii. $0.10101111\cdots$
   iv. $0.11000\cdots$
   v. $0.101111\cdots$.

   (c) Pruebe que todo real del intervalo $]0, 1]$ que posea un desarrollo binario periódico con período cero, también posee un desarrollo binario (único) periódico con período uno.

5.4 LOS NÚMEROS COMPLEJOS.

Los complejos hicieron su aparición dentro de las matemáticas debido a la necesidad de poseer un campo numérico en el cual ecuaciones tan simples como $x^2+1=0$ y $x^2+x+1=0$ tuviesen solución.

En un principio fueron manipulados por los matemáticos con suma desconfianza, por pura necesidad y por no creer que "existiesen verdaderamente"; de ahí el nombre de "parte imaginaria" que aún subsiste hoy en día.

Con el tiempo el conjunto de los números complejos vino a ser más o menos

$$C=\{a+bi \mid a,b\in\mathbb{R}\},$$

donde el "+" era el símbolo de una suma formal e "i" representaba una de las soluciones de $x^2=-1$; se les manejaba formalmente según las reglas usuales de la aritmética y muchas veces dicho manejo sólo se hacía como puente entre resultados concernientes a números reales.

Los prejuicios que se tenían se quedaron sin fundamento cuando en 1833 el matemático irlandés Sir William R. Hamilton los logró construir a partir de los números reales, como parejas ordenadas de éstos, dotados de adición y multiplicación definidas convenientemente.

Es en esencia el desarrollo que vamos a bosquejar solamente, debido a lo conocido del tratamiento y a la abundante y asequible literatura que existe sobre el tema; se encuentra en casi cualquier texto de algebra elemental o de variable compleja.

La idea central está en que dos complejos $a+bi$ y $c+di$ son iguales si y solamente si $a=c$ y $b=d$, lo cual equivale a la igualdad entre las parejas ordenadas (a,b) y (c,d). En consecuencia, un complejo debe ser simplemente una pareja ordenada de números reales, es decir

$$\mathbb{C}=\mathbb{R}\times\mathbb{R}=\{(a,b)\mid a,b\in\mathbb{R}\}.$$

La adición y la multiplicación se definen en la forma:

$$(a,b)+(c,d)=(a+c,b+d)$$
$$(a,b)\cdot(c,d)=(ac-bd,ad+bc)$$

El por qué de tales definiciones se halla fácilmente si se piensa en que la primera componente es la parte real y la segunda es la parte imaginaria del

complejo.

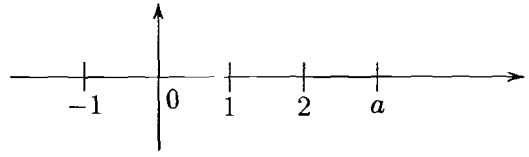
$$([a+bi]+[c+di]=[a+c]+[b+d]i \quad \text{y}$$
$$[a+bi][c+di]=ac+bd(i)^2+adi+dci$$
$$=[ac-bd]+[ad+bc]i.$$

Es cuestión de rutina demostrar sus propiedades fundamentales:

TEOREMA 15. *La adición en $\mathbb{C}$ es conmutativa, asociativa, modulativa e invertiva. La multiplicación en $\mathbb{C}-\{0\}$ es asociativa, modulativa e invertiva. Además la multiplicación es distributiva con respecto a la adición.*

Como ayuda para el lector que quiera probarlo por sí mismo: el módulo de la adición es $(0,0)$, el inverso aditivo de (a,b) es $(-a,-b)$, el módulo de la multiplicación es $(1,0)$ y si $(a,b)\neq(0,0)$, su inverso multiplicativo es $(a/[a^2+b^2],-b/[a^2+b^2])$, el cual también puede hallarse como solución de $(a,b)\cdot(x,y)=(1,0)$.

Cuando tomamos un sistema de coordenadas cartesianas en el plano, generalmente identificamos al eje de las equis con los números reales:



Puede verse que esta identificación es en realidad un isomorfismo de $\mathbb{R}$ sobre los complejos con la segunda coordenada nula: Sea $\widehat{\mathbb{R}}=\{(a,0)\mid a\in\mathbb{R}\}$ y sea $f:\mathbb{R}\longrightarrow\mathbb{C}$ dada por $f(a)=(a,0)$; con sólo efectuar sencillas operaciones se comprueba que

$$f(a)+f(b)=(a,0)+(b.0)=(a+b,0)=f(a+b) \quad \text{y}$$
$$f(a)\cdot f(b)=(a,0)\cdot(b,0)=(a\cdot b,0)=f(a\cdot b).$$

Así $\mathbb{C}$ posee un subconjunto $\widehat{\mathbb{R}}$, que es un campo isomorfo con $\mathbb{R}$; podemos identificarlo con $\mathbb{R}$ y en vez de $(a,0)$ escribir simplemente a.

PROPOSICIÓN 21. $(a,b)=(a,0)+(b,0)\cdot(0,1)$.

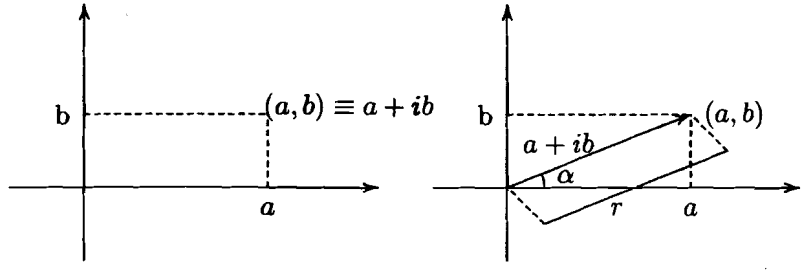
Demostración. Efectuar las operaciones indicadas. □

Además, $(0,1)\cdot(0,1)=(-1,0)=-1$ (recuérdese la identificación hecha), es decir que el cuadrado de $(0,1)$ es -1, razón por la cual notaremos po i al complejo $(0,1)$. Con esta convención, la proposición 21 se transforma en

$$(a,b)=(a,0)+(b,0)\cdot(0,1)$$
$$=a+bi,$$

llegándose a la forma usual.

Los complejos construidos de esta manera pueden verse como puntos en un plano provisto de un sistema cartesiano de coordenadas o también como vectores que van del origen a los puntos del plano.



La suma de los complejos previamente definida coincide entonces con la suma de vectores del plano e inclusive el producto puede interpretarse gráficamente cuando los complejos se ven como vectores determinados por su dirección y su longitud: si r es la longitud, $r = \sqrt{a^2 + b^2}$, y α el ángulo que forma con el semieje positivo de las equis, $a = r\cos\alpha$, $b = r\,sen\,\alpha$ y $a + bi = r(\cos\alpha + i sen\,\alpha)$, a la cual se le llama *forma trigonométrica* del complejo; entonces,

$$r(\cos\alpha + i sen\,\alpha)\cdot s(\cos\beta + i sen\,\beta) = rs(\cos(\alpha+\beta) + i sen\,(\alpha+\beta))$$

como puede comprobarse efectuando las operaciones y teniendo en cuenta la forma de expresar *coseno* y *seno* de la suma de ángulos; gráficamente lo anterior significa que el producto es un vector con longitud igual al producto de las longitudes de los factores y con ángulo igual a la suma de los ángulos de los factores.

Combinando la anterior forma de multiplicar complejos con la inducción matemática, se obtiene el llamado teorema de De Moivre:

$$[r(\cos\alpha + i sen\,\alpha)]^n = r^n[\cos(n\alpha) + i sen\,(n\alpha)].$$

A un complejo ω le llamamos una *raíz enésima* del complejo z si y sólo si $\omega^n = z$. Expresando a z en su forma trigonométrica $z = r(\cos\alpha + i sen\,\alpha)$ y buscando también a ω en su forma trigonométrica $\omega = s(\cos\varphi + i sen\,\varphi)$, el teorema de De Moivre nos permite concluir $s = r^{1/n}$ y $\varphi = \dfrac{\alpha + 2\pi k}{n}$, es decir que las raíces enésimas se obtienen cuando a k se le dan los ene valores $0, 1, 2, \cdots, n-1$ en $\omega = r^{1/n}(\cos\dfrac{\alpha+2\pi k}{n} + i sen\,\dfrac{\alpha+2\pi k}{n})$.

Aun cuando al conjunto de los complejos se le puede ordenar totalmente de muchas maneras, ninguna de ellas lo transforma en un campo ordenado,

o sea que para ninguna relación de orden total de $\mathbb{C}$ se cumplen las propiedades de monotonía de la adición y de la multiplicación, como se puede demostrar por contradicción: Supongamos que existe un orden total "$\prec$" de $\mathbb{C}$ tal que

$$(\forall z_1, z_2, \omega \in \mathbb{C})(z_1 \prec z_2 \longrightarrow z_1 + \omega \prec z_2 + \omega) \tag{1}$$

$$\text{y } (\forall z_1, z_2, \omega \in \mathbb{C})(z_1 \prec z_2 \wedge 0 \prec \omega \longrightarrow z_1\omega \prec z_2\omega). \tag{2}$$

Es fácil demostrar que

$$(\forall z \in \mathbb{C})[z \neq 0 \longrightarrow (0 \prec z) \veebar (0 \prec -z)] \tag{3}$$

$$\text{y } (\forall z_1, z_2, \omega \in \mathbb{C})[(z_1 \prec z_2) \wedge (\omega \prec 0) \longrightarrow z_2\omega \prec z_1\omega]\ . \tag{4}$$

Se deduce inmediatamente de (2) y (4) que

$$(\forall z \in \mathbb{C})(z \neq 0 \rightarrow z^2 \prec 0) \tag{5}$$

En particular, $1 = 1^2 \succ 0$ y por (3) se sigue $-1 \prec 0$

Pero también de (5) se obtiene que $(i)^2 \succ 0$, es decir $-1 \succ 0$ (contradicción).

Ejercicios

1. Demuestre en detalle el teorema 15.
2. Exprese en su forma trigonométrica a los complejos $1 - \sqrt{3}i$, $2 + 2i$, 4, -2, i, $-5i$, $-1 + \sqrt{3}i$.
3. Usando el teorema de De Moivre calcule $(1 - \sqrt{3}i)^8$.
4. Halle las cuatro raíces cuartas de 1.
5. Resuelva las ecuaciones
   (a) $z^2 - 1 = 0$.
   (b) $z^2 + 1 - \sqrt{3}i = 0$.
   (c) $z^3 + i = 0$.

6. Demuestre que si $n \in \mathbb{N}$, $(i)^n = i^r$, siendo $0 \leq r < 4$ el residuo que se obtiene al dividir a n por 4.

7. Definiendo para z complejo las potencias en la forma $z^0 = 1$ y $z^{n+1} = z^n \cdot z$ para todo z, y $z^{-n} = \frac{1}{z^n}$ para $z \neq 0$ y $n \in \mathbb{N}$, demuestre que $z^n z^m = z^{m+n}$, $(z^n)^m = z^{(mn)}$ y $(z\omega)^n = z^n \omega^n$, donde z y ω no pueden ser cero cuando sus exponentes no sean positivos.

8. Halle $\sqrt{-3+4i}$ sin usar la fórmula dada, sino escribiendo

$$\sqrt{-3+4i} = a + bi$$

y elevando al cuadrado e igualando partes reales y partes imaginarias respectivas y resolviendo las ecuaciones resultantes.

(a) Demuestre que para la ecuación de segundo grado

$$az^2 + bz + c = 0 \quad \text{con} \quad a, b, c \in \mathbb{C} \quad \text{y} \quad a \neq 0.$$

también es válida la fórmula usual

$$z = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

(Se ha suprimido el $\pm$ porque es innecesario al existir dos raíces cuadradas del complejo $b^2 - 4ac$).

(b) Halle las soluciones de $4z^2 + 4(1+i)z + (3-2i) = 0$.

9. Demuestre el teorema de De Moivre.

10. Deduzca rigurosamente la fórmula para hallar las ene raíces enésimas de un complejo.

**

Capítulo 6

CONJUNTOS INFINITOS Y CARDINALES

Deseamos poner de presente en este capítulo las primeras ideas sobre el tamaño de los conjuntos infinitos, usando como medida del tamaño precisamente su número de elementos.

6.1 CONJUNTOS INFINITOS

En la sección 2 del capítulo IV se definió un conjunto finito como aquel cuyo número de elementos es un natural y el concepto "infinito" se tomó como la simple negación de "finito", o sea que un conjunto A es infinito si no existe un natural n tal que A sea equipotente con $\{0, 1, \cdots, n-1\}$.

En la presente sección introduciremos una forma de comparar tamaños de conjuntos y estableceremos dos resultados intuitivamente simples, pero formalmente difíciles de probar: todo conjunto finito posee estrictamente menos elementos que $\mathbb{N}$ y todo conjunto infinito tiene mayor o igual cantidad de elementos que $\mathbb{N}$.

Antes vimos que dos conjuntos poseen igual cantidad de elementos cuando son equipotentes, o sea cuando sus elementos se pueden poner en correspondencia biunívoca; si al tratar de establecer una tal correspondencia entre A y B sobrasen elementos en B, es decir B poseyera mayor (o igual) cantidad de elementos que A, sólo se obtendría una función inyectiva de A en B. En consecuencia,

DEFINICIÓN 1. *Diremos que el conjunto A* es dominado *por el conjunto*

B (o que B domina *a A) para significar que existe una función inyectiva de A en B. En tal caso escribiremos $A \preceq B$ ó $B \succeq A$.*

Nótese que "A es dominado por B" es equivalente a "A es equipotente con un subconjunto de B", puesto que si $f : A \to B$ es inyectiva, al restringir el codominio al recorrido se obtiene $f : A \to f(A)$ biyectiva de modo que $A \approx f(A) \subseteq B$ y recíprocamente si $A \approx A'$ y $A' \subseteq B$, existe una biyección $g : A \to A'$ y al componerla con la inyección canónica $i : A' \to B$ (i(x)=x) se obtiene una inyección de A en B.

En particular si $A \subseteq B$, entonces $A \preceq B$ ya que $A \approx A$.

Es trivial comprobar que si $A \approx B$, entonces $A \preceq B \wedge B \preceq A$.

PROPOSICIÓN 1. *La relación de dominación es reflexiva y transitiva, es decir $A \preceq A$ cualquiera sea A y para A, B, C, conjuntos cualesquiera,*

$$(A \preceq B \wedge B \preceq C) \to (A \preceq C).$$

Demostración. Para cualquier conjunto A su aplicación idéntica $I_A : A \to A$ es biyectiva, en particular inyectiva, de modo que $A \preceq A$.

Si $A \preceq B \wedge B \preceq C$, A es equipotente con el subconjunto A' de B y existe $g : B \to C$ inyectiva; su restricción $g : A' \to g(A')$ es una biyección, luego $A' \approx g(A') \subseteq C$ y siendo $A \approx A'$, la transitividad de la equipotencia permite concluír $A \approx g(A') \subseteq C$, o sea $A \preceq C$. □

PROPOSICIÓN 2.

a) *Si $A' \approx A \wedge A \preceq B$, entonces $A' \preceq B$,*

b) *Si $A \preceq B \wedge B \approx B'$, entonces $A \preceq B'$.*

Demostración. Es inmediata y la dejamos al lector. □

Supongamos $A \approx B$ y $A \neq B$; existe una biyección $f : A \to B$ y su inversa $f^{-1} : B \to A$ también es una biyección; siendo las dos en particular inyectivas se cumple que $A \preceq B$ y $B \preceq A$.

Esto hace ver que "$\preceq$" no es antisimétrica: $(A \preceq B) \wedge (B \preceq A) \wedge (A \neq B)$. Sin embargo posee una propiedad sustitutiva:

TEOREMA 1. Teorema de Cantor-Bernstein.

$$Si \quad A \preceq B \quad y \quad B \preceq A, \quad entonces \quad A \approx B.$$

Existen muchas pruebas de este resultado, algunas de las cuales son muy complicadas. Nos permitimos presentar, con ligeras modificaciones y algunas explicaciones adicionales, una demostración realizada por los matemáticos G. Birkhoff y H. MacLane; es elegante, sencilla y fácil de comprender.

Sean $f : A \to B$ y $g : B \to A$ inyectivas; podemos suponer sin pérdida de generalidad que $A \cap B = \emptyset$[1] y que ninguna de las dos funciones es sobreyectiva ya que si alguna lo fuese se tendría inmediatamente la equipotencia deseada.

Queremos construir una función biyectiva $F : A \to B$; la táctica será la siguiente: Descompondremos cada uno de los conjuntos A y B en tres subconjuntos disyuntos dos a dos y hallaremos biyecciones entre tales subconjuntos, las cuales al ser reunidas darán como resultado (ver el corolario 2 del teorema 10 del capítulo III) la biyección deseada.

Puesto que f y g son inyectivas, se obtienen a partir de ellas restricciones biyectivas al tomar como codominios a los respectivos recorridos, de modo que $f^{-1} : f(A) \to A$ y $g^{-1} : g(B) \to B$ son funciones también biyectivas.

Sea $x \in A$; si $x \in g(B)$, entonces $g^{-1}(x)$ existe y le llamaremos el primer *ancestro* de x (el nombre se debe a que $g^{-1}(x)$ genera a x mediante g). Si $g^{-1}(x) \in f(A)$, $f^{-1}(g^{-1}(x))$ existe y será llamado el segundo ancestro de x; si $f^{-1}(g^{-1}(x)) \in g(B)$, entonces $g^{-1}(f^{-1}(g^{-1}(x)))$ existe y será llamado el tercer ancestro de x; si continuamos el proceso de hallar los ancestros cuarto, quinto, etc., se presentan tres casos:

1. x tiene un número par de ancestros; esto significa que x posee un último ancestro a en A, el cual no tiene primer ancestro (es decir $a \notin g(B)$). Notemos por A_p al subconjunto de A formado por aquellos elementos de A que poseen un número par de ancestros (recuerde el lector que cero es par).

2. x tiene un número impar de ancestros, lo cual significa que x posee un último ancestro b en B con $b \notin f(A)$. Notemos por A_I al subconjunto de A formado por tales elementos.

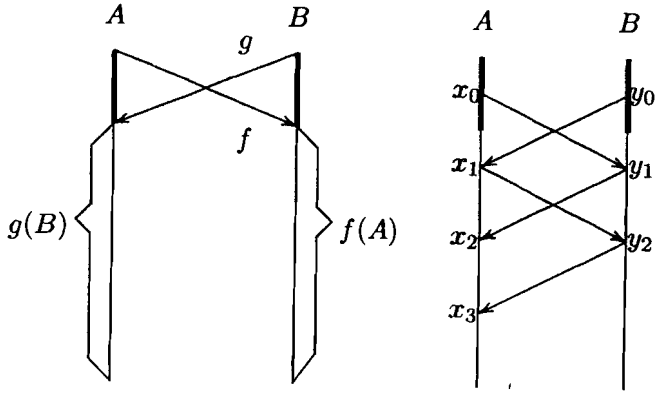
3. x tiene infinitos ancestros. Notemos por A_∞ a la colección de aquellos elementos de A que poseen infinitos ancestros.

   Los tres subconjunto A_p, A_I y A_∞ son disyuntos dos a dos y su unión es A.

[1] Si A y B poseen elementos en común, existen $A' = A \times \{0\}$ y $B' = B \times \{1\}$ equipotentes respectivamente con A y B y disyuntos, los cuales pueden reemplazar a A y a B (según la proposición 2) en el teorema.

De la misma manera descomponemos B en los subconjuntos B_p, B_I y B_∞, disyuntos dos a dos y con unión igual a B.

En el gráfico que sigue x_i es un elemento de A con i ancestros y y_k es un elemento de B con k ancestros; las flechas están en el sentido de las respectivas funciones directas.



Si $x \in A$ posee infinitos ancestros, evidentemente $f(x)$ también los posee; si $y \in B_\infty$, su primer ancestro $a = f^{-1}(b)$ también tiene infinitos ancestros. Esto prueba que la restricción (de f) $f_1 : A_\infty \to B_\infty$ está bien definida y es sobreyectiva; es además inyectiva por serlo f.

Si $x \in A_p$, su imagen $f(x) \in B$ y posee un ancestro más, es decir $f(x) \in B_I$; recíprocamente si $y \in B_I$, por lo menos tiene un primer ancestro x, el cual evidentemente está en A_p y es tal que $f(x) = y$. Se concluye que $f_2 : A_p \to B_I$ dada por $f_2(x) = f(x)$ es una restricción biyectiva de f.

Finalmente, si $x \in A_I$, por lo menos tiene un primer ancestro $g^{-1}(x)$ en B, el cual obviamente está en B_p, de modo que se puede restringir g^{-1} correctamente para obtener $g_*^{-1} : A_I \to B_p$, la cual es inyectiva por serlo g^{-1} y es además sobreyectiva ya que si $y \in B_p$ entonces su imagen $g(y) = x$ está en A_I (tiene un ancestro más que y) y $g^{-1}(x) = y$.

La demostración está completa puesto que como se dijo antes,

$$F = f_1 \cup f_2 \cup g_*^{-1} : A = A_\infty \cup A_p \cup A_I \to B_\infty \cup B_I \cup B_p = B$$

es biyectiva.

Dada la importancia del teorema de *Cantor-Bernstein*, y para ilustrar las formas tan diferentes como puede resolverse un problema en matemáticas, vamos a dar a continuación una nueva demostración de este teorema:

LEMA DEL PUNTO FIJO. *Sea A un conjunto arbitrario no vacío y $h : \mathcal{P}(A) \to \mathcal{P}(A)$ una función creciente con respecto a "$\subseteq$", es decir, tal que si $X_1 \subseteq X_2$, entonces $h(X_1) \subseteq h(X_2)$.*

Sea $\mathfrak{C} = \{X \in \mathcal{P}(A) | X \subseteq h(X)\}$. Entonces el conjunto $T = \bigcup_{X \in \mathfrak{C}} X$ es un punto fijo de h, es decir, satisface la condición $h(T) = T$.

Demostración. Sea $X \in \mathfrak{C}$; por definición de T es claro que $X \subseteq T$; por hipótesis $h(X) \subseteq h(T)$ y por definición de $\mathfrak{C}$, $X \subseteq h(X)$, luego $X \subseteq h(T)$ y en consecuencia (Ejercicio 3, sección 5, cap. I)

$$T = \bigcup_{X \in \mathfrak{C}} X \subseteq h(T). \tag{1}$$

Aplicando h se obtiene $h(T) \subseteq h(h(T))$, o sea que $h(T) \in \mathfrak{C}$, de donde

$$h(T) \subseteq \bigcup_{X \in \mathfrak{C}} X = T \tag{2}$$

De (1) y (2) se concluye que $h(T) = T$, como queríamos probar.

Sean A, B, f, g como en el enunciado del teorema de Cantor-Bernstein y en el primer párrafo de la prueba dada antes. Para construir la biyección $F : A \to B$, descompondremos a cada uno de estos conjuntos en dos subconjuntos disyuntos y estableceremos biyecciones entre ellos:

Consideremos la función $h : \mathcal{P}(A) \to \mathcal{P}(A)$ definida en la forma siguiente: $h(X) = A - g(B - f(X))$ para todo $X \in \mathcal{P}(A)$.

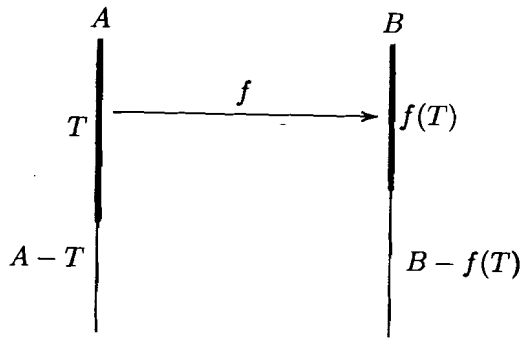
Sean X_1, X_2 subconjuntos de A tales que $X_1 \subseteq X_2$; por el ejercicio 6 a), sección 3, Cap III, $f(X_1) \subseteq f(X_2)$, luego sus complementos cumplen la relación recíproca; $B - f(X_2) \subseteq B - f(X_1)$ y aplicando g,

$$g(B - f(X_2)) \subseteq g(B - f(X_1))$$

y tomando complementos, $A - g(B - f(X_1)) \subseteq A - g(B - f(X_2))$ es decir, $h(X_1) \subseteq h(X_2)$, de modo que h satisface la hipótesis del lema del punto fijo. Por lo tanto si $\mathfrak{C} = \{X \in \mathcal{P}(A) | X \subseteq h(X)\}$ y $T = \bigcup_{X \in \mathfrak{C}} X$, entonces $T = h(T) = A - g(B - f(T))$, de donde $g(B - f(T)) = A - T$.

Así $g_1 : B - f(T) \to A - T$, restricción de g, es una biyección (ya que g es inyectiva por hipótesis) y su inversa $g_1^{-1} : A - T \to B - f(T)$ también

lo será.



Como f es inyectiva, su restricción $f_1 : T \to f(T)$ es así mismo una biyección, luego

$$F = f_1 \cup f_2 : T \cup (A - T) = A \longrightarrow f(T) \cup (B - f(T)) = B$$

es la biyección deseada. □

Es el momento de introducir el concepto de dominación estricta:

DEFINICIÓN 2. *$A \prec B$ significa $A \preceq B \wedge \neg(A \approx B)$.*

Es entonces intuitivamente cierta la equivalencia siguiente:

PROPOSICIÓN 3. *$A \prec B$ si y sólo si $A \preceq B \wedge \neg(B \preceq A)$.*

Demostración Probemos que las conjunciones $A \preceq B \wedge \neg(A \approx B)$ y $A \preceq B \wedge \neg(B \preceq A)$ son equivalentes; como de cada una de ellas se deduce $A \preceq B$, es suficiente ver que de cada una de las conjunciones se deduce la segunda proposición de la otra.

Si $A \preceq B \wedge \neg(B \preceq A) \wedge (A \approx B)$, entonces $A \preceq B \wedge \neg(B \preceq A) \wedge (B \preceq A)$ lo cual es contradictorio de manera que cuando $A \preceq B \wedge \neg(B \preceq A)$ se deberá tener necesariamente $\neg(A \approx B)$.

Análogamente, si $A \preceq B \wedge \neg(A \approx B) \wedge (B \preceq A)$, entonces por el teorema 1, $A \approx B \wedge \neg(A \approx B)$ (contradictorio), luego cada vez que $A \preceq B \wedge \neg(A \approx B)$ también se tendrá $\neg(B \preceq A)$. □

PROPOSICIÓN 4.

a) *Si $(A' \approx A) \wedge (A \prec B)$ entonces $A' \prec B$.*

b) *Si $(A \prec B) \wedge (B \approx B')$, entonces $A \prec B'$.*

Sus demostraciones son realmente sencillas y las dejamos al lector.

PROPOSICIÓN 5. *Si $A \preceq B$ y $B \preceq C$ y una de las dos dominaciones es estricta, entonces $A \prec C$.*

Demostración. Siendo la dominación transitiva, $A \preceq C$, de modo que es suficiente probar $\neg(A \approx C)$; si no se tuviese, o sea que si $A \approx C$, la parte a) de la proposición 2 implicaría $C \preceq A$ y la parte b) de la misma proposición, $B \preceq A$, es decir $A \preceq B$ y $B \preceq A$ y $B \preceq C$ y $C \preceq B$, de donde por el teorema 1, $A \approx B$ y $B \approx C$ y ninguna de las dominaciones sería rigurosa, quedando demostrado. □

COROLARIO 1. *La dominación estricta es transitiva.*

PROPOSICIÓN 6. *Para todo número natural n se tiene que $n \prec \mathbb{N}$.*

Demostración. Es una consecuencia inmediata de los ejercicios 10 y 11 de la sección 2 del capítulo IV. □

Ya sabemos que $\mathbb{N}$ es infinito; se tienen además los resultados que siguen:

PROPOSICIÓN 7. *Si un conjunto A es finito, entonces $A \prec \mathbb{N}$.*

Demostración. Si A es finito, existe n natural tal que $A \approx n$; como $n \prec \mathbb{N}$, la proposición 4 permite concluir $A \prec \mathbb{N}$. □

TEOREMA 2. (Teorema Fundamental). *Todo conjunto infinito posee un subconjunto equipotente con $\mathbb{N}$.*

Demostración. Sea A un conjunto infinito, es decir, $\neg(\exists n \in \mathbb{N})(A \approx n)$, o sea $(\forall n \in \mathbb{N})(\neg(A \approx n))$.

Como A no es equipotente con cero, A no es vacío, luego $\exists x_0(x_0 \in A)$

Como $\neg(A \approx \{0\} = 1)$, entonces $(A - \{x_0\}) \neq \emptyset$, o lo que es lo mismo, $\exists x_1(x_1 \in (A - \{x_0\}))$.

Como $\neg(A \approx \{0,1\} = 2)$, claramente $A - \{x_0, x_1\} \neq \emptyset$, de modo que $\exists x_2(x_2 \in (A - \{x_0, x_1\}))$.

Como $\neg(A \approx \{0,1,2\})$, claramente $A - \{x_0, x_1, x_2\} \neq \emptyset$, luego existe x_3 en $A - \{x_0, x_1, x_2\}$.

Repitiendo este argumento *infinitas* veces, tantos como números naturales, se obtiene una sucesión $x_0, x_1, x_2, \cdots$ de elementos distintos de A, ya que cada uno es diferente de todos los que le preceden; en otras palabras, la función $f : \mathbb{N} \to A$ definida por $f(n) = x_n$ es inyectiva, luego $\mathbb{N} \approx f(\mathbb{N}) = \{x_0, x_1, x_2, \dots\} \subseteq A$, quedando demostrado.[2] □

[2]Ver comentarios al comienzo de la sección siguiente.

De los tres últimos renglones es claro que:

COROLARIO 2. *Si A es infinito, $A \succeq \mathbb{N}$.*

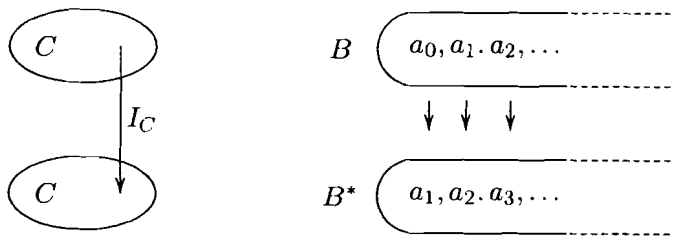
COROLARIO 3. *Si $A \prec \mathbb{N}$, entonces A es finito.*

Demostración. Si $A \prec \mathbb{N}$ y A fuese infinito, por el corolario 1 se tendría $A \prec \mathbb{N}$ y $\mathbb{N} \preceq A$, de donde por la proposición 5, $A \prec A$ (contradicción). □

COROLARIO 4. *Si A es infinito, entonces A es equipotente con alguno de sus subconjuntos propios.*

Demostración. En el capítulo III se vio que $\mathbb{N}$ es equipotente con $\mathbb{N}^*$ usando la función de $\mathbb{N}$ en $\mathbb{N}$ dada por $f(n) = n + 1$; algo semejante se hace en el caso general.

Sea A infinito; por el teorema 2, A posee un subconjunto equipotente con $\mathbb{N}$, digamos $B = \{a_0, a_1, a_2, \dots\}$; sea $C = A - B$. Si $A^* = A - \{a_0\}$ y $B^* = B - \{a_0\}$, también $C = A^* - B^*$, o sea que A es la unión disyunta de B y C y también A^* es la unión disyunta de B^* y C; sea $f_1 : B \to B^*$ definida por $f_1(a_n) = a_{n+1}$ y sea I_C la identidad de C; nuevamente el corolario del teorema 10 del capítulo III permite concluir que $f_1 \cup I_C : B \cup C :\to B^* \cup C$ es una biyección, de modo que $A = B \cup C \approx B^* \cup C = A^*$ y claramente A^* es un subconjunto propio de A. □



TEOREMA 3. *Un conjunto es infinito si y sólo si es equipotente con alguno de sus subconjuntos propios.*

Demostración. Después del corolario 3, sólo hace falta ver que si un conjunto es equipotente con alguno de sus subconjuntos propios, entonces es infinito, lo cual es equivalente a su contrarrecíproca, "si es finito, entonces con ninguno de sus subconjuntos propios es equipotente", proposición ya demostrada en el capítulo IV (Prop 15). □

Cuando $p \longleftrightarrow q$, también $\neg p \longleftrightarrow \neg q$, de modo que además se tiene: *Un conjunto es finito* si y sólo si *no posee un subconjunto propio con el cual sea equipotente.*

Esta propiedad se toma algunas veces como definición de conjunto finito, caso en el cual se llama "finitud en el sentido de Dedekind" por haber sido propuesta por él.

Al concepto de finitud introducido en la definición del capítulo IV se le llama entonces "finitud en el sentido ordinario". Hemos demostrado la equivalencia de las dos definiciones, merced al teorema 2.

Ejercicios

1. Complete (si falta algo) los desarrollos de la sección anterior para concluir que un conjunto A es infinito si y sólo si $A \succeq \mathbb{N}$.

2. La proposición 7 y el corolario 2 del teorema 2 se juntan para obtener que "un conjunto A es finito si y sólo si $A \prec \mathbb{N}$".

   ¿Se hubiese podido obtener este resultado con sólo negar a ambos lados del "si y sólo si" en la proposición del ejercicio 1. anterior? Dé las razones de su respuesta.

3. Use un técnica semejante a la empleada en la demostración del corolario 3 del teorema 2 para probar que si A es infinito, entonces para cualquier B finito, $B \subseteq A$, se tiene que $A \approx (A - B)$.

4. Demuestre que el teorema 1 (Cantor-Bernstein) es equivalente al enunciado siguiente: Si X, Y, Z son conjuntos cualesquiera tales que $X \subseteq Y \wedge Y \subseteq Z \wedge X \approx Z$, entonces $X \approx Y$.

5. Pruebe que todo subconjunto infinito de $\mathbb{N}$ es equipotente con $\mathbb{N}$.

6. Demuestre que si $(A \approx B) \wedge (C \approx D) \wedge (A \cap C = \emptyset = B \cap D)$, entonces $A \cup C \approx B \cup D$.

7. Pruebe que si $(A \approx B) \wedge (C \approx D)$, entonces $A \times C \approx B \times D$ y que si $X \preceq Y$, entonces $(X \times Z) \preceq (Y \times Z)$ y que si $(X \preceq Y) \wedge (M \preceq N)$, entonces $(X \times M) \preceq (Y \times N)$.

8. Demuestre que $A \times B \approx B \times A$ y que $A \times (B \times C) \approx (A \times B) \times C$.

9. Revise las definiciones y compruebe que $A \preceq B$ si y sólo si $(A \prec B) \veebar (A \approx B)$.

6.2 FORMAS DEL AXIOMA DE ELECCIÓN

Al finalizar la sección 4 del capítulo III se vio que si B es un conjunto infinito cualquiera y $f : A \to B$ es sobreyectiva mas no inyectiva, para obtener una restricción biyectiva g de f tal que $\mathcal{R}(g) = \mathcal{R}(f) = B$, se debía formar el conjunto $f_u = \{(x,y) \in f \mid y = u\}$ para cada elemento u de B, y luego elegir de cada uno de los f_u una única pareja ordenada; se dijo que nunca concluiríamos esta labor aun cuando pasásemos toda nuestra vida en tal empeño, ya que se deben hacer infinitas elecciones de parejas.

En la sección anterior de este capítulo, para probar que todo conjunto infinito posee un subconjunto numerable, el argumento fue más o menos el siguiente: Sea A infinito;

0) $A \neq \emptyset$, luego existe $a_0 \in A$;

1) $A - \{a_0\} \neq \emptyset$, luego existe $a_1 \in A - \{a_0\}$;

2) $A - \{a_0, a_1\} \neq \emptyset$, luego existe $a_2 \in A - \{a_0, a_1\}$;

3) $A - \{a_0, a_1, a_2\} \neq \emptyset$, luego existe $a_3 \in A - \{a_0, a_1, a_2\}$;

$\vdots$

Repitiendo este raciocinio tantas veces como números naturales existen, se obtiene una sucesión $a_0, a_1, a_2, \ldots$ de elementos distintos de A, los cuales constituyen un subconjunto numerable de A.

La demostración anterior, tan clara y sencilla, no es considerada como una deducción realizada a partir de los axiomas que hemos dado, aduciéndose nuevamente como argumento las limitaciones que le imponen al hombre su misma finitud, por las cuales éste no puede repetir un proceso infinitas veces; se dice que necesitaría un período infinito de tiempo y que una deducción o procedimiento lógico debe terminar en un lapso finito de tiempo.

Si rechazamos de plano la posibilidad de realizar elecciones de infinitos objetos en finito tiempo, tampoco tendrían soluciones problemas tan sencillos como el siguiente, ideado por Bertrand Russell:

Imaginemos un conjunto cuyos elementos son pares de zapatos, tantos pares como números naturales. ¿Es el conjunto de todos estos pares equipotente con el conjunto de todos los zapatos que forman los pares? La

respuesta es afirmativa y puede establecerse la biyección fácilmente: Al primer par hagamos corresponder el zapato derecho del primer par; al segundo par el zapato izquierdo del primer par; al tercer par hagamos corresponder el zapato derecho del segundo par, al cuarto par el zapato izquierdo del segundo par, y *así sucesivamente*; este "así sucesivamente" se puede precisar: cualquiera sea $n \geq 1$, el zapato derecho del enésimo par se lo hacemos corresponder al par $2n-1$ y el zapato izquierdo del enésimo par corresponderá al par $2n$. Evidentemente esta regla define la biyección deseada.

La situación cambia completamente si en vez de zapatos suponemos que se tiene pares de medias; la diferencia está en que los fabricantes producen medias idénticas para los dos pies. Ciertamente podemos comenzar asignando al primer par una media arbitraria de este par, al segundo par la otra media del primer par, al tercer par una media arbitraria del segundo par, y así sucesivamente, Pero aquí no disponemos de una regla que nos permita establecer la biyección deseada y sólo podremos continuar este proceso finitas veces.

A no ser que estemos dispuestos a admitir un nuevo principio que nos coloque en capacidad de realizar al menos teóricamente infinitas elecciones simultáneas, no podremos demostrar que el conjunto de todas las medias es equipotente al de los pares de medias.

Los dos problemas expuestos anteriormente no tendrían solución sin la posibilidad de poder efectuar infinitas elecciones en un período corto de tiempo.

Las elecciones de infinitos objetos son inherentes a la naturaleza de la misma matemática; por ejemplo la función $y = x^2$ de $\mathbb{R}$ en $\mathbb{R}$ no es otra cosa que un conjunto de infinitas elecciones, tantas como números reales, ya que por cada x real se está eligiendo otro

real (su cuadrado) para formar la pareja ordenada (x, x^2) de la función; también la frase "el menor elemento de A" es simplemente la descripción de infinitas elecciones, ya que de cada subconjunto no vacío A de $\mathbb{N}$ se está eligiendo un elemento su menor. Claro está que en estos dos casos poseemos un *regla* que nos permite efectuar la elección de una manera constructiva, o sea que tal regla proporciona instrucciones precisas que permiten de manera unívoca elegir el correspondiente objeto en un período finito de tiempo.

Precisamente el nuevo axioma tiene como fin *permitirnos suponer que podemos efectuar infinitas elecciones simultáneas de objetos* cuando tales reglas no existen. Podemos asegurar que en esta forma se perfecciona la estructura de la Matemática al poderse manejar más cómodamente los conjuntos infinitos a pesar de nuestra aparente finitud.

Algunos autores arguyen además que el pensamiento es instantáneo, que no requiere tiempo medible, que por ejemplo en dos minutos podríamos efectuar tantas elecciones como números naturales, siempre y cuando gastásemos 1 minuto en la primera, medio minuto en la segunda, 1/4 en la tercera, 1/8 en la cuarta, $\cdots$, $\frac{1}{2^{n-1}}$ en la enésima, etc. Que por tal motivo debemos admitir un principio que refleje nuestra estructura mental en ese sentido, permitiéndonos elegir infinitos objetos en un lapso finito de tiempo. A dicho principio se le acostumbra llamar el *axioma de elección* y puede enunciarse como sigue:

AE : *A toda colección $\mathfrak{C}$ no vacía de conjuntos no vacíos, corresponde al menos un función e de dominio $\mathfrak{C}$ tal que para todo A de $\mathfrak{C}$, $e(A) \in A$.*

Se dice que e es una función de elección para $\mathfrak{C}$, ya que al ser $e(A)$ elemento de A, se puede interpretar como aquel que e elige de A.

En particular, si X es un conjunto no vacío y $\mathcal{P}_0(X)$ es la colección de partes no vacías de X, existe una función $e : \mathcal{P}_0 \to X$ tal que $e(A) \in A$ para todo subconjunto A de X; se acostumbra decir que e es una función de elección para X. Es fácil ver que el axioma de elección es equivalente a

AE' : *Para todo conjunto no vacío existe una función de elección.*

Si éste se cumple y $\mathfrak{C}$ es una colección no vacía de conjuntos no vacíos, sea $X = \cup\mathfrak{C}$; entonces $\mathfrak{C} \subseteq \mathcal{P}_0(X)$ y si e es una función de elección para X, su restricción a $\mathfrak{C}$ es la función pedida en AE.

Una tercera forma ligeramente diferente del axioma de elección, pero históricamente la primera, es la siguiente, propuesta por Ernst Zermelo en 1904:

PZ (Postulado de Zermelo): *Si $\mathfrak{C}$ es una colección no vacía de conjuntos no vacíos y disyuntos dos a dos, entonces existe al menos un conjunto E tal que $E \subseteq \cup\mathfrak{C}$ y para todo $C \in \mathfrak{C}$, $E \cap C$ es unitario.*

Como PZ se deduce inmediatamente de AE, probemos que también AE se deduce de PZ: Sea $\mathfrak{C}$ es una colección no vacía de conjuntos no vacíos; sea $\mathfrak{C}^* = \{\{A\} \times A \mid A \in \mathfrak{C}\}$. Como $(\{A\} \times A) \approx A$, entonces $\mathfrak{C}^*$ es una colección no vacía de conjuntos no vacíos y disyuntos dos a dos (compruébelo, amigo lector), luego por el postulado de Zermelo existe E tal que $E \cap (\{A\} \times A)$ es unitario para todo A, es decir para cada A de $\mathfrak{C}$, el conjunto E tan sólo

posee una pareja (A, a) con a en A, o sea que E es una función, precisamente la función de elección deseada.

Necesitamos introducir alguna terminología adicional para presentar el axioma de elección bajo un nuevo ropaje lingüístico.

Como dice Paul R. Halmos (ver [5], p.53), hay casos en los cuales se considera el recorrido de una función como más importante que la función misma; cuando esto sucede, tanto el vocabulario como la notación cambian; supóngase que este es el caso para una función $f : I \to X$; en vez de determinar la función mediante su correspondiente conjunto de parejas ordenadas $\{(i, f(i)) \mid i \in I\}$, se acostumbra usar la notación $(f(i))_{i\in I}$ y con mayor frecuencia $(x_i)_{i\in I}$, entendiéndose que $x_i = f(i)$. Se dice entonces que $(x_i)_{i\in I}$ *es una familia de elementos de* X *con índices en* I; al dominio I se le llama el conjunto de índices y cuando $I \neq \emptyset$ se dice que la familia es no vacía.

Por ejemplo una familia $(x_i)_{i\in \mathbb{N}}$ es simplemente una sucesión; una tripla ordenada (x_1, x_2, x_3) puede verse como una familia $(x_i)_{i\in\{1,2,3\}}$, es decir, como una función de dominio $\{1, 2, 3\}$. Análogamente una énupla ordenada $(x_1, x_2, \cdots, x_n)$ no es más que una familia $(x_i)_{i\in I}$ con $I = \{1, 2, \cdots, n\}$. Estos ejemplos ponen de presente que si A_1, A_2, A_3 son conjuntos cualesquiera, su producto $A_1 \times A_2 \times A_3 = \{(x_1, x_2, x_3) | x_1 \in A_1 \wedge x_2 \in A_2 \wedge x_3 \in A_3\}$ no es otra cosa que $\{(x_i)_{i\in\{1,2,3\}} \mid (\forall i \in \{1, 2, 3\})(x_i \in A_i)\}$ y que si además A_1, A_2, A_3 son no vacíos, podemos escoger x_1 en A_1, x_2 en A_2 y x_3 en A_3 para formar una tripla ordenada (x_1, x_2, x_3), concluyéndose que en este caso $A_1 \times A_2 \times A_3$ no es vacío.

Siguiendo esta idea es posible extender la definición de producto cartesiano: Si $(A_i)_{i\in I}$ es una familia cualquiera de conjuntos, su producto cartesiano se define como

$$\prod_{i\in I} A_i = \{(x_i)_{i\in I} \mid (\forall i \in I)(x_i \in A_i)\}.$$

o sea como la colección de todas las familias $(x_i)_{i\in I}$ que pueden formarse escogiendo el i-ésimo elemento x_i en el i-ésimo conjunto A_i .

Si $\prod_{i\in I} A_i \neq \emptyset$ y $(x_i)_{i\in I}$ es uno de sus elementos, como $x_i \in A_i$ cualquiera sea i, la función $e(A_i) = x_i$ es en realidad una función de elección para los conjuntos de la familia, de manera que el axioma de elección se puede enunciar también en la forma siguiente:

AE" : *El producto cartesiano de una familia no vacía de conjuntos no vacíos, no es vacío.*

Probemos su equivalencia con PZ: Supongamos PZ y sea $(A_i)_{i\in I}$ una familia no vacía de conjuntos no vacíos; para cada i en I, sea $A_i^* = \{i\} \times A_i$; A_i^* no es vacío y si $i \neq j$, $A_i^* \cap A_j^* = \emptyset$ de modo que si $\mathfrak{C}$ es el conjunto de los A_i^* (es decir si $\mathfrak{C}$ es el recorrido de la función definida por la familia $(A_i^*)_{i\in I}$), entonces $\mathfrak{C}$ es una colección no vacía de conjuntos no vacíos y disyuntos dos a dos, de modo que por PZ existe un conjunto $E \subseteq \cup\mathfrak{C}$ tal que $\forall A_i^* \in \mathfrak{C}$, $E \cap A_i^* = \{(i, x_i)\}$, o sea que para cada i de I tan sólo existe en E una pareja (i, x_i) con x_i en A_i; de manera que E es la función buscada de I en $\cup A_i$, es decir, $E = (x_i)_{i\in I}$ es elemento de $\prod_{i\in I} X_i$ y este es no vacío.

Recíprocamente, supongamos AE" y probemos AE: Sea $\mathfrak{C}$ una colección no vacía de conjuntos no vacíos; su aplicación idéntica $f : \mathfrak{C} \to \mathfrak{C}$ (con $f(C) = C$) la transforma en una familia con índices en sí misma $(C_C)_{C\in\mathfrak{C}}$, siendo $C_C = C$, luego su producto cartesiano $\prod_{C\in\mathfrak{C}} C_C$ no es vacío y si $e = (x_C)_{C\in\mathfrak{C}}$ es uno de sus elementos, $e(C) = x_C \in C_C = C$ y e es la función de elección buscada.

Para ilustrar un poco más la forma como se trabaja con este axioma, vamos a deducir algunos resultados de cierta utilidad.

PROPOSICIÓN 8. *Toda relación incluye una función con el mismo dominio, es decir, si* R *es una relación, existe una función* $f \subseteq R$ *tal que* $\mathcal{D}(f) = \mathcal{D}(R)$.

Demostración. Sea R una relación no vacía (el caso $R = \emptyset$ es trivial); para cada $a \in \mathcal{D}(R)$ el conjunto $\{(x, y) \in R \mid x = a\} = \mathcal{D}_a$ no es vacío, luego $\mathfrak{C} = \{\mathcal{D}_a \mid a \in \mathcal{D}(R)\}$ es una colección no vacía de conjuntos no vacíos disyuntos dos a dos; por PZ existe un conjunto $E \subseteq \cup\mathcal{D}_a = R$ tal que $E \cap \mathcal{D}_a = \{(a, y)\}$ para cada a en $\mathcal{D}(R)$, de modo que E es una función que cumple las condiciones exigidas. □

La proposición 8 también es equivalente al axioma de elección: Sea $\mathfrak{C}$ una colección no vacía de conjuntos no vacíos; entonces para toda A de $\mathfrak{C}$ el conjunto $\{A\} \times A$ es no vacío; la unión $R = \bigcup_{A\in\mathfrak{C}}(\{A\} \times A)$ es una relación de dominio $\mathfrak{C}$, la cual debe contener una función e con el mismo dominio, siendo ésta necesariamente de elección por la forma como se construyó R.

Otro aspecto útil del axioma de elección es el relacionado con la existencia de funciones inversas laterales de funciones no biyectivas. Un primer resultado, independiente del axioma de elección es el siguiente:

PROPOSICIÓN 9. *Si* $f : A \to B$ *es inyectiva y* $A \neq \emptyset$, *existe* $g : B \to A$ *sobreyectiva tal que* $g \circ f = I_A$.

Demostración. Sea $f : A \to B$ inyectiva; $f : A \to f(A)$ es biyectiva luego f^{-1} es una biyección de $f(A)$ sobre A y basta extenderla a todo B, lo cual se logra uniendo a f^{-1} el conjunto $\{(y, a) \mid y \in (B - f(A))\}$, donde a es un elemento fijo de A; es evidente que la función g así obtenida es sobreyectiva y tal que $g \circ f = I_A$. □

Un segundo resultado, en realidad equivalente al axioma de elección, es el siguiente:

PROPOSICIÓN 10. *Si $A \neq \emptyset$ y $f : A \to B$ es sobreyectiva, existe $g : B \to A$ inyectiva tal que $f \circ g = I_B$.*

Demostración. Sea $f : A \to B$ sobreyectiva; para cada b de B sea $f_b = \{(x, y) \in f \mid y = b\}$; los conjuntos f_b son no vacíos; (f es sobre) y disyuntos dos a dos, luego AE" aplicado a $C = \{f_b \mid b \in B\}$ produce un conjunto u contenido en f tal que $u \cap f_b$ es unitario para toda b en B, luego $u : \mathcal{D}(u) \to \mathcal{R}(u) = B$ es una restricción biyectiva maximal de f (se resuelve así el problema considerado al comienzo de la presente sección), luego $u^{-1} : B \to \mathcal{D}(u)$ es también biyectiva y al componerla con la inyección canónica $j : \mathcal{D}(u) \to A$ obtenemos la inyección g deseada. □

De las dos proposiciones anteriores se deduce en particular que:

TEOREMA 4. *Sean A y B conjuntos no vacíos. Existe una función inyectiva $f : A \to B$ si y sólo si existe una función $g : B \to A$ sobreyectiva.*

Para terminar esta sección vamos a demostrar rigurosamente que "*Todo conjunto infinito posee un subconjunto numerable*":

Sea X un conjunto infinito y sea e una función de elección con dominio $\mathcal{P}(X) - \{\emptyset\}$; notemos por $\mathfrak{F}$ a la colección de todos los subconjuntos finitos de X.

Seguiremos las mismas ideas usadas en la primera demostración, con la ayuda adicional que representa poseer una función e que ya ha elegido un elemento de cada subconjunto no vacío de X.

Como X es infinito, si A es cualquiera de sus subconjuntos finitos, $X - A \neq \emptyset$, pudiéndose calcular $e(X - A)$; este elemento no está en A puesto que $e(X - A) \in (X - A)$ por ser e de elección, de manera que $A \cup \{e(X - A)\}$ tiene realmente un elemento más que A, siendo éste un subconjunto propio de aquel.

Si definimos $g : \mathfrak{F} \to \mathfrak{F}$ mediante $g(A) = A \cup \{e(X - A)\}$, entonces A es un subconjunto propio de $g(A)$ y éste tiene un elemento más que A, de manera que si comenzamos con el conjunto vacío y aplicamos g repetidas

veces, $g(\emptyset)$ tendrá un elemento, $g(g(\emptyset))$ tendrá dos, etc. El teorema de la definición por recurrencia nos permite expresar de manera rigurosa esta idea: Para $g : \mathfrak{F} \to \mathfrak{F}$ y $\emptyset$ en $\mathfrak{F}$, existe una única función $\mu : \mathbb{N} \to \mathfrak{F}$ tal que $\mu(0) = \emptyset$ y $\mu(n+1) = g(\mu(n))$. Veamos más en detalle cómo es esta función μ:

$$\begin{aligned}
\mu(1) = g(\mu(0)) &= g(\emptyset) = \emptyset \cup \{e(X - \emptyset)\} \\
&= \{e(X)\} = \{x_0\} \quad \text{tomando} \quad x_0 = e(X). \\
\mu(2) = g(\mu(1)) &= \mu(1) \cup \{e(X - \mu(1))\} \\
&= \{x_0\} \cup \{e(X - \{x_0\})\} = \{x_0, x_1\} \\
&\text{tomando} \quad x_1 = e(X - \{x_0\}). \\
\mu(3) = g(\mu(2)) &= \mu(2) \cup \{e(X - \mu(2))\} \\
&= \{x_0, x_1\} \cup \{e(X - \{x_0, x_1\})\} = \{x_0, x_1, x_2\} \\
&\text{tomando} \quad x_2 = e(X - \{x_0, x_1\}) \in (X - \{x_0, x_1\}).
\end{aligned}$$

$$\vdots$$

y en general,

$$\begin{aligned}
\mu(n+1) &= \mu(n) \cup \{e(X - \mu(n))\} \\
&= \{x_0, x_1, \cdots, x_{n-1}\} \cup \{e(X - \mu(n))\} \\
&= \{x_0, x_1, \cdots, x_{n-1}, x_n\}
\end{aligned}$$

tomando $x_n = e(X - \mu(n)) = e(X - \{x_0, x_1, \cdots, x_{n-1}\})$, el cual está en $X - \{x_0, x_1, \ldots, x_{n-1}\}$ y es por consiguiente distinto de todos los x_i con $i < n$, luego si $m \neq n$, por la tricotomía del orden $(m < n) \veebar (n < m)$ y en cualquier caso $x_m \neq x_n$.

Se concluye que la función $f : \mathbb{N} \to X$ definida mediante $f(n) = x_n$ (o sea $e(X - \mu(n))$) es inyectiva, luego $\mathbb{N} \approx f(\mathbb{N}) \subseteq X$, obteniéndose el resultado deseado.

Ejercicios

1. Demuestre que la proposición 10 anterior implica el Postulado de Zermelo.
   Ayuda: Si $\mathfrak{C}$ es una colección no vacía de conjuntos no vacíos y disyuntos dos a dos, $\bigcup_{A \in \mathfrak{C}} (A \times \{A\})$ es una función de $\cup \mathfrak{C}$ *sobre* $\mathfrak{C}$.

2. Si $(A_i)_{i\in I}$ es una familia de conjuntos (es decir, una función de dominio I), la *unión de la familia* se define como la unión de las imágenes, o sea

$$\bigcup_{i\in I} A_i = \{x \mid (\exists i \in I)(x \in A_i)\}.$$

Análogamente si $I \neq \emptyset$,

$$\bigcap_{i\in I} A_i = \{x \mid (\forall i \in I)(x \in A_i)\}.$$

Demuestre que:

$$M \cup (\bigcap_{i\in I} A_i) = \bigcap_{i\in I}(M \cup A_i).$$
$$M \cap (\bigcup_{i\in I} A_i) = \bigcup_{i\in I}(M \cap A_i).$$
$$M \times (\bigcup_{i\in I} A_i) = \bigcup_{i\in I}(M \times A_i).$$
$$M \times (\bigcap_{i\in I} A_i) = \bigcap_{i\in I}(M \times A_i).$$

3. Sean $f : B \to C$ y $g : A \to C$ tales que $\mathcal{R}(f) \subseteq \mathcal{R}(g)$. Pruebe que existe una función $h : B \to A$ tal que $g \circ h = f$.

4. ¿Es el enunciado "Toda función posee una restricción biyectiva maximal" equivalente al axioma de elección? Dé las razones de su respuesta.

6.3 CONJUNTOS CONTABLES

Son aquellos conjuntos con a lo más tantos elementos como el conjunto de los números naturales; nos proponemos demostrar que el conjunto de los números racionales (aun cuando para algunos lectores sea difícil de creer) es contable.

DEFINICIÓN 3. *Diremos que un conjunto es contable si y sólo si es dominado por el de los números naturales, es decir, A es contable si y sólo si $A \preceq \mathbb{N}$.*

DEFINICIÓN 4. *Un conjunto se llamará numerable si y sólo si es equipotente con $\mathbb{N}$.*

Según el ejercicio 9 de la sección 1, A es contable si y sólo si $(A \prec \mathbb{N}) \veebar (A \approx \mathbb{N})$, o sea si y sólo si A es finito o numerable.

Nótese entonces que si un conjunto es contable y no es finito, deberá ser numerable; como usaremos con frecuencia este hecho, lo destacaremos: *Un conjunto contable e infinito es numerable.*

PROPOSICIÓN 11.

a) *Todo conjunto equipotente con uno contable es contable.*

b) *Todo conjunto equipotente con uno numerable es también numerable.*

c) *Entre dos conjuntos numerables, siempre existe al menos una biyección del uno en el otro.*

d) *Si A es contable y B es numerable, entonces existe al menos una inyección de A en B.*

Demostración. Las partes b) y c) son consecuencias inmediatas de la simetría y la transitividad de la equipotencia y las a) y d) se siguen de la proposición 2. □

PROPOSICIÓN 12. *Todo subconjunto infinito de un conjunto numerable es numerable.*

Demostración. Es prácticamente igual a la del ejercicio 5 de la sección 1 anterior y no la haremos para que el lector ponga algo de su parte. □

PROPOSICIÓN 13. *Todo subconjunto de un conjunto contable es contable.*

Demostración. Como $A \subseteq B \rightarrow A \preceq B$, es una consecuencia inmediata de la transitividad de la dominación. □

Trivialmente $\mathbb{N}$ y $\mathbb{N}^*$ son numerables; también lo son según la Proposición 12, el conjunto de los naturales pares $\{0,2,4,5,\cdots\}$ y el de los impares $\{1,3,5,7,\cdots\}$. Más interesante es ver que $\mathbb{Z}$ también es numerable; la función definida mediante el diagrama siguiente es una biyección.

$$\begin{array}{cccccccccccc} \{\ldots, & -5, & -4, & -3, & -2, & -1, & 0, & 1, & 2, & 3, & 4, \ldots\} = \mathbb{Z} \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \{\ldots, & 9, & 7, & 5, & 3, & 1, & 0, & 2, & 4, & 6, & 8, \ldots\} = \mathbb{N} \end{array}$$

Para el lector que crea que las funciones sólo se definen por "fórmulas", la anterior función $f : \mathbb{Z} \rightarrow \mathbb{N}$ se puede determinar así:

$$\begin{aligned} f(n) &= 2n \quad \text{si} \quad n \geq 0 \qquad (f : \mathbb{Z} \rightarrow \mathbb{N}) \\ &= -2n-1 \quad \text{si} \quad n < 0 \end{aligned}$$

Es decir que

f_1 : Enteros no negativos $\rightarrow$ Naturales Pares, con $f_1(n) = 2n$ y
f_2 : Enteros negativos $\rightarrow$ Impares, con $f_2(n) = -2n-1$,

son biyecciones con dominios y codominios disyuntos de modo que su unión $f = f_1 \cup f_2$ es también una biyección. Nuevamente la proposición 9 pone de presente que los conjuntos $\{2n \mid n \in \mathbb{Z}\}$ y $\{2n+1 \mid n \in \mathbb{Z}\}$ de enteros pares e impares respectivamente, son numerables, lo mismo que $\mathbb{Z}^* = \mathbb{Z} - \{0\}$. Vayamos hacia la numerabilidad de conjuntos mayores.

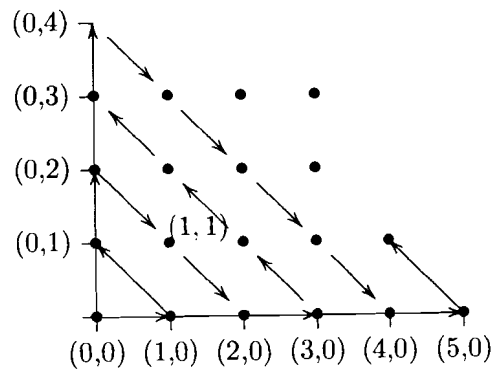
TEOREMA 5. $\mathbb{N} \times \mathbb{N}$ *es numerable.*

Primera Demostración: Como la función $\mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ definida mediante $n \rightarrow (n,0)$ es trivialmente inyectiva, entonces $\mathbb{N} \preceq (\mathbb{N} \times \mathbb{N})$; si logramos probar que $(\mathbb{N} \times \mathbb{N}) \preceq \mathbb{N}$, el teorema de Cantor-Bernstein nos permite concluir inmediatamente que $\mathbb{N} \approx \mathbb{N} \times \mathbb{N}$. Para obtener $(\mathbb{N} \times \mathbb{N}) \preceq \mathbb{N}$, es suficiente hallar una función $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ inyectiva. Una manera de hacerlo es tomar dos naturales mayores que 1 que sean primos relativos, por ejemplo 2 y 3 y definir f en la forma $f(m,n) = 2^m \cdot 3^n$; es fácil probar que f es inyectiva; si $f(m,n) = f(p,q)$, $2^m \cdot 3^n = 2^p \cdot 3^q$, pero 2^m divide a $2^m 3^n$, luego 2^m divide a $2^p 3^q$ y siendo 2 primo con 3, 2^m divide a 2^p, de modo que $m \leq p$. Intercambiando los papeles en el argumento anterior, $m = p$ y utilizando la propiedad cancelativa del producto en la igualdad inicial se deduce $3^n = 3^q$, luego $n = q$ y $(m,n) = (p,q)$. □

Segunda demostración. Que un conjunto sea numerable significa que podemos disponer sus elementos en sucesión infinita sin repeticiones de elementos, ya que si $f : \mathbb{N} \rightarrow A$ es biyectiva, entonces

$$A = \{f(0), f(1), f(2), \cdots\} = \{a_0, a_1, a_2, \cdots\}.$$

con $a_i \neq a_j$ cuando $i \neq j$. Se dice que ésta es una *numeración biyectiva* de A.

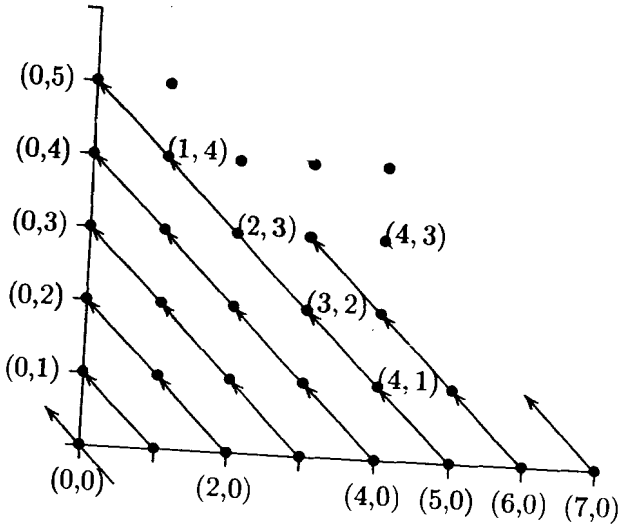


Representemos gráficamente $\mathbb{N} \times \mathbb{N}$ y tracemos una sucesión de flechas, las cuales determinan la numeración (en forma diagonal) de los elementos de $\mathbb{N} \times \mathbb{N}$, como lo muestra el gráfico adjunto.

El gráfico puede interpretarse intuitivamente como un cordel que va pasando por los puntos de $\mathbb{N} \times \mathbb{N}$, es decir, sobre el cual se van marcando los puntos de $\mathbb{N} \times \mathbb{N}$; si lo estirásemos, estos aparecerían exactamente como uno marca los puntos de $\mathbb{N}$ sobre una semirrecta con origen incluido.

La estrategia con que se recorre todo $\mathbb{N} \times \mathbb{N}$ fue creada por G. Cantor y es uno de sus famosos procedimientos diagonales. Puede modificarse para producir una biyección f de $\mathbb{N} \times \mathbb{N}$ sobre $\mathbb{N}$ y convencer categóricamente al más escéptico. Simplemente cambiamos el orden del recorrido, conservando

la diagonalidad:



Comenzamos en $(0,0)$ (o sea que $f(0,0)=0$) y pasamos a $(1,0)$ y seguimos a $(0,1)$ (o sea que $f(1,0)=1$ y $f(0,1)=2$); saltamos a $(2,0)$ y continuamos a $(1,1)$ y a $(0,2)$ (o sea que $f(2.0)=3$, $f(1,1)=4$, $f(2,0)=5$); saltamos a $(3,0),\cdots$

Si convenimos que "$(0,0)$ está sobre la diagonal cero", entonces $(0,1)$ y $(1,0)$ están en la diagonal 1, y $(2,0)$, $(1,1)$ y $(0,2)$ están en la diagonal $2,\cdots$. Observamos que todos los puntos (x,y) de la diagonal n son tales que $x+y=n$ y que la diagonal n está constituida por $n+1$ puntos.

Así para averiguar el sitio que ocupa en la sucesión un punto (x,y) (comenzando a contar por 1), sumamos $x+y$; así (x,y) está en la diagonal $x+y$; sobre las diagonales anteriores hay $1+2+3+\cdots+(x+y)$ puntos; en la diagonal $x+y$, el punto (x,y) ocupa el lugar $y+1$, luego el punto (x,y) está en el lugar $1+2+3+\cdots+(x+y)+(y+1)$ (comenzando a contar por 1), o sea $\frac{(x+y)(x+y+1)}{2}+y+1$; si comenzamos a contar por cero, (x,y) estará en el lugar $\frac{(x+y)(x+y+1)}{2}+y$, es decir que $f(x,y)=\frac{(x+y)(x+y+1)}{2}+y$ es la biyección de $\mathbb{N}\times\mathbb{N}$ sobre $\mathbb{N}$ que estábamos buscando. □

COROLARIO 5. $\mathbb{Z}\times\mathbb{Z}^*$ *es numerable.*

Demostración. Como $\mathbb{Z}\approx\mathbb{N}$ y $\mathbb{Z}^*\approx\mathbb{N}$, entonces (ejercicio 7 de la sección 1 anterior) $\mathbb{Z}\times\mathbb{Z}^*\approx\mathbb{N}\times\mathbb{N}\approx\mathbb{N}$. □

A primera vista $\mathbb{Z}\times\mathbb{Z}^*$ es mucho más numeroso que $\mathbb{Q}$, ya que los racionales son clases de equivalencia de elementos de $\mathbb{Z}\times\mathbb{Z}^*$ y hay menos clases de

equivalencia que elementos de $\mathbb{Z}\times\mathbb{Z}^*$; esto implica que $\mathbb{Q}\preceq\mathbb{Z}\times\mathbb{Z}^*$ y siendo $\mathbb{Z}\times\mathbb{Z}^*$ numerable, $\mathbb{Q}$ será contable, pero por ser infinito $\mathbb{Q}$ resultará numerable.

Para obtener realmente este resultado basta establecer de una manera rigurosa que $\mathbb{Q}\preceq\mathbb{Z}\times\mathbb{Z}^*$, para lo cual es suficiente demostrar que $\mathbb{Q}$ es equipotente con un subconjunto (infinito) de $\mathbb{Z}\times\mathbb{Z}^*$.

Sea $\widehat{\mathbb{Q}}=\{(0,1)\}\cup\{(m,n)\in\mathbb{Z}\times\mathbb{Z}^*\mid n>0\wedge m \text{ primo relat. con } n\}$.

Evidentemente $\widehat{\mathbb{Q}}$ es un subconjunto infinito ($\forall k\in\mathbb{Z}$, $(k,1)\in\widehat{\mathbb{Q}}$) de $\mathbb{Z}\times\mathbb{Z}^*$ y en consecuencia numerable.

La función $f:\widehat{\mathbb{Q}}\to\mathbb{Q}$ dada por $f(m,n)=\frac{m}{n}$ es una biyección puesto que $f(0,1)=0$ y para $m\neq 0$ se tiene que $\frac{m}{n}$ no es otra cosa que la forma irreducible de un racional y es conocido que todo racional no nulo posee una única forma irreducible.

Enunciémoslo formalmente:

TEOREMA 6. *El conjunto de los racionales es numerable.*

Sabemos que un conjunto A es contable si y sólo si existe una función inyectiva $f:A\to\mathbb{N}$; pero según el teorema 4, esto sucede si y sólo si existe una función sobreyectiva $g:\mathbb{N}\to A$. En esta forma obtenemos una estrategia alternativa para demostrar que un conjunto es contable: construir una función de $\mathbb{N}$ sobre A. Mejor aún:

TEOREMA 7. *Un conjunto A es contable si y sólo si dado cualquier conjunto B numerable, existe una función de B sobre A.*

Demostración. Como B es numerable, hay una biyección $h:B\to\mathbb{N}$. Si A es contable, existe una función sobreyectiva $g:\mathbb{N}\to A$; la compuesta $g\circ h:B\to\mathbb{N}$ es la función sobreyectiva buscada. Recíprocamente si existe $f:B\to A$ sobreyectiva, la compuesta $f\circ h^{-1}$ es una función de $\mathbb{N}$ sobre A, luego A es contable. □

Como una aplicación del teorema 7, demostraremos nuevamente que $\mathbb{Q}$ es contable: Sabemos que $\mathbb{Z}\times\mathbb{Z}^*$ es numerable, de manera que basta hallar una función de $\mathbb{Z}\times\mathbb{Z}^*$ sobre $\mathbb{Q}$. La más natural es aquella que a toda pareja (m,n) hace corresponder el racional m/n. Contrasta esta prueba tan sencilla con la anterior para la cual utilizamos la unicidad de la representación de un racional como m/n con m y n primos relativos.

Como un corolario más del teorema 5 se tiene el resultado siguiente:

PROPOSICIÓN 14. *Si $A_1,A_2,\cdots A_n$ ($n\geq 2$) son conjuntos contables, su producto cartesiano también es contable.*

Demostración.

a) Si A_1 y A_2 son contables, $A_1 \preceq \mathbb{N}$ y $A_2 \preceq \mathbb{N}$, luego por la última parte del ejercicio 7 de la sección 1, $(A_1 \times A_2) \preceq (\mathbb{N} \times \mathbb{N})$, y siendo $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$, por la proposición 2 concluimos que $A_1 \times A_2 \preceq \mathbb{N}$.

b) Supongamos que la propiedad vale para n y mostremos que también se tiene para $n+1$:

$$A_1 \times A_2 \times \cdots \times A_n \times A_{n+1} = (A_1 \times A_2 \times \cdots \times A_n) \times A_{n+1}$$

y este último producto es contable ya que tanto $A_1 \times A_2 \times \cdots \times A_n$ como A_{n+1} lo son, y por la parte a) la propiedad se cumple para dos. □

Observemos que si todos los conjuntos son finitos, su producto también lo es (proposición 22, Cap IV) y si todos los conjuntos son no vacíos y al menos uno es numerable, su producto cartesiano será infinito y en consecuencia numerable.

De suma utilidad son los dos resultados siguientes:

PROPOSICIÓN 15. *La unión de una colección numerable de conjuntos contables disyuntos dos a dos es contable.*

Demostración. Sea $\{A_0, A_1, A_2, \cdots\}$ una numeración biyectiva fija de la colección numerable $\mathfrak{C}$ de conjuntos contables disyuntos dos a dos; como cada uno de los A_k es contable, dispongamos sus elementos en una sucesión fija, $A_k = \{a_{k0}, a_{k1}, a_{k2}, \cdots\}$ (finita o no según lo sea A_k). Definamos una función $f : \bigcup_{n\in\mathbb{N}} A_n \to \mathbb{N}\times\mathbb{N}$ en la forma siguiente: Sea $x \in \bigcup_{n\in\mathbb{N}} A_n$; como los A_n son disyuntos dos a dos, existe un único k tal que $x \in A_k$; entonces $x = a_{kj}$ con k, j únicos. Definimos $f(x) = (k, j)$ haciéndole corresponder la pareja ordenada de sus subíndices (x pertenece al conjunto k-ésimo y en él ocupa el j-ésimo lugar). Claramente f está bien definida ya que los conjuntos son disyuntos dos a dos y además es inyectiva (si $x \neq y$, difieren en el conjunto al cual pertenecen, o si están en el mismo, difieren en el lugar que ocupan en la sucesión). Entonces $\bigcup_{n\in\mathbb{N}} A_n \preceq \mathbb{N}\times\mathbb{N}$ y como $\mathbb{N}\times\mathbb{N} \approx \mathbb{N}$, entonces por la proposición 2, $\bigcup_{n\in\mathbb{N}} A_n \preceq \mathbb{N}$. □

Una forma más técnica de hacer esta prueba es la siguiente: Debido a que cada uno de los A_n es contable, cada A_n es equipotente con un subconjunto $\hat{A}_n$ de $\mathbb{N}$; si $D_n = \{n\} \times \hat{A}_n$, trivialmente $\hat{A}_n \approx D_n$ y por transitividad, $A_n \approx D_n$. Existe entonces una biyección $f_n : A_n \to D_n$; siendo disyuntos

dos a dos tanto los dominios de las f_n como los codominios, su unión es una biyección $f = \bigcup_{n\in\mathbb{N}} f_n : \bigcup_{n\in\mathbb{N}} A_n \to \bigcup_{n=\in\mathbb{N}} D_n$.[3] Como $\hat{A}_n \subseteq \mathbb{N}$, $\{n\} \times \hat{A}_n = D_n \subseteq \{n\} \times \mathbb{N}$ luego $\bigcup_{n\in\mathbb{N}} D_n \subseteq \bigcup_{n\in\mathbb{N}} \{n\} \times \mathbb{N} = \mathbb{N} \times \mathbb{N}$ o sea que f establece una equipotencia entre $\bigcup_{n\in\mathbb{N}} A_n$ y un subconjunto de $\mathbb{N} \times \mathbb{N}$, lo cual prueba que $\bigcup_{n\in\mathbb{N}} A_n$ es contable (por las proposiciones 11 y 13).

El mismo argumento sirve para el caso en el cual la familia en vez de numerable es finita, luego "la unión de una colección contable de conjuntos contables disyuntos dos a dos es contable".

La condición de ser disyuntos dos a dos se puede eliminar, ya que de no serlo, la unión posee intuitivamente menos elementos que en el caso de ser disyuntos.

TEOREMA 8. *La unión de cualquier colección contable de conjuntos contables es también contable.*

Demostración. Como la colección $\{A_0, A_1, \cdots A_n\}$ posee la misma unión que la colección numerable $\{A_0, A_1, A_2 \ldots, A_n, \emptyset, \emptyset, \emptyset, \ldots\}$, basta considerar el caso numerable. Sea $\{A_0, A_1, A_2 \ldots\}$ una colección numerables de conjuntos contables; definamos una nueva colección numerable así: $B_0 = A_0$, $B_1 = A_1 - A_0$, $B_2 = A_2 - (A_0 \cup A_1)$ y en general $B_n = A_n - \left(\bigcup_{k=0}^{n-1} A_k\right)$; se observa que $B_n \subseteq A_n$, así que los B_n son contables y disyuntos dos a dos; además $\bigcup_{n=0}^{\infty} A_n = \bigcup_{n=0}^{\infty} B_n$ (el lector debe probar estas dos afirmaciones; vea el ejercicio 9 de la sección 5 del Cap. I), siguiéndose inmediatamente el teorema por la proposición 15. □

Como un ejemplo de su aplicación probemos nuevamente que $\mathbb{Q}$ es contable; para cada n entero mayor que cero, sea $\mathbb{Z}_n = \{\frac{p}{n} \mid p \in \mathbb{Z}\}$: trivialmente $\mathbb{Z}_n \approx \mathbb{Z}$, así que $\mathbb{Z}_n$ es numerable. Por el teorema 8, $\bigcup_{n=1}^{\infty} \mathbb{Z}_n$ es contable, pero esta unión es precisamente $\mathbb{Q}$, así que éste es contable; siendo infinito, es numerable.

Combinando este resultado con la proposición 14 se obtiene que también $\mathbb{Q} \times \mathbb{Q}$, $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$ y en general $\mathbb{Q}^n$, son contables.

Terminemos esta sección ilustrando la forma como se puede manipular un conjunto infinito y demostrando el teorema 8 usando funciones sobreyectivas.

[3] Ver ejercicio 12 de la sección 3 del Cap III.

Mostremos que $\mathbb{N}$ puede descomponerse en infinitos subconjuntos infinitos disyuntos dos a dos: Como A_0 tomemos el conjunto de los impares:

$$A_0 = \{1, 3, 5, 7, 9, 11, \cdots\} = \{2n+1 \mid n \in \mathbb{N}\} \approx \mathbb{N}$$

obtengamos A_1 multiplicando por 2 todos los números de A_0:

$$A_1 = \{2, 6, 10, 14, 18, 22, \cdots\} = \{2(2n+1) \mid n \in \mathbb{N}\} \approx \mathbb{N}$$

En general,

$$A_k = \{2^k(2n+1) \mid n \in \mathbb{N}\} \approx \mathbb{N} \quad .$$

Claramente todos los A_k son numerables y $\bigcup_{k=0}^{\infty} A_k = \mathbb{N} - \{0\} = \mathbb{N}^*$. Además si $i \neq k$, necesariamente $A_i \cap A_k = \emptyset$ ya que la descomposición de un natural no nulo en la forma $2^k(2m+1)$ es única (ver ejercicio 4, sección 7, Cap. III).

Si $(C_k)_{k\in\mathbb{N}}$ es una familia numerable de conjuntos contables, por el teorema 7 existe para cada k una función $f_k : A_k \to C_k$ sobreyectiva. Como los A_k son disyuntos dos a dos, $\bigcup_{k=0}^{\infty} f_k$ es una función de $\mathbb{N}^* = \bigcup_{k=0}^{\infty} A_k$ en $\bigcup_{k=0}^{\infty} C_k$ también sobreyectiva. (ejercicio 12, sección 3, Cap. III), luego de nuevo por el teorema 7 se concluye que $\bigcup_{k=0}^{\infty} C_k$ es contable.

Ejercicios

1. Pruebe que $(\forall n \in \mathbb{N}^*)(\mathbb{Z}^n$ es numerable).

2. Notemos por $\mathbb{Z}[x]$ al conjunto de todos los polinomios en x con coeficientes enteros, es decir, $\mathbb{Z}[x]$ está formado por todos los elementos de la forma $a_0 + a_1x + a_2x^2 + \cdots a_nx^n$, donde $a_0, a_1, \cdots a_n$ son enteros. Demuestre que $\mathbb{Z}[x]$ es numerable.

   Ayuda: Si $\mathbb{Z}_n[x]$ designa al subconjunto de $\mathbb{Z}[x]$ formado por todos los polinomios de grado menor o igual a n, pruebe que $\mathbb{Z}_n \approx \mathbb{Z}^{n+1}$ y use el ejercicio 1. Observe además que $\mathbb{Z}[x] = \bigcup_{n=1}^{\infty} \mathbb{Z}_n[x]$ y use el teorema 8.

3. Para cada $p(x)$ en $\mathbb{Z}[x]$, sea $P = \{\omega \in \mathbb{C} \mid p(\omega) = 0\}$, es decir, P es el conjunto de las soluciones de la ecuación $p(x) = 0$. Use el teorema fundamental del álgebra para concluir que P es finito. Emplee el teorema 8 para deducir que

$$A = \{\omega \in \mathbb{C} \mid (\exists p(x) \in \mathbb{Z}[x])(p(\omega) = 0)\}$$

es numerable.

Tal conjunto es el de todas las soluciones de todas las ecuaciones polinomiales; se le llama *el conjunto de los números algebraicos.* Al conjunto $A \cap \mathbb{R}$ se le dice el de los reales algebraicos; a un elemento de $\mathbb{R} - A$ se le llama un número *real trascendente*; ¿podría el lector dar un ejemplo de uno de tales

números?

4. Sea n un natural positivo fijo; si $r \in \mathbb{R}^+$ y $P \in \mathbb{R}^n$, llamamos *"n-disco abierto de centro en P y radio r"* al conjunto de todos los puntos de $\mathbb{R}^n$ que distan de P menos que r.

$$D(P, r) = \{X \in \mathbb{R}^n : \|P - X\| < r\}$$

Dibuje un n-disco en los casos $n = 1, 2, 3$.

Decimos que un n-disco es racional si su radio es un número racional y si todas las coordenadas de su centro son números racionales.

Pruebe que el conjunto de todos los n-discos racionales es numerable. Ayuda: Muestre que es equipotente con $\mathbb{Q}^{n+1}$.

5. Demuestre que toda colección de n-discos disyuntos dos a dos es contable. Ayuda: Sea $\mathfrak{C}$ una colección tal; $\mathbb{Q}^n \cap (\bigcup_{\mathfrak{C}} \mathfrak{C})$ es numerable; halle una función de este conjunto sobre $\mathfrak{C}$.

6.

   (a) Notemos D_n al conjunto de los decimales entre 0 y 1 que poseen n cifras, es decir, $D_0 = \{0\}$ y para $n \geq 1$,

   $$D_n = \{0.a_1a_2 \cdots a_n \mid a_1, a_2, \cdots, a_n \in \{0, 1, 2 \cdots, 9\} \wedge a_n \neq 0\}.$$

   Pruebe que D_n es finito y calcule su número de elementos.

   (b) Demuestre que el conjunto D de todos los decimales finitos mayores o iguales que cero y menores o iguales que 1 es numerable. Ayuda: $D = \bigcup_{n\in\mathbb{N}} D_n$.
   Análogamente, si se usara el sistema de numeración binario, y si $B_0 = \{0\}$ y $B_n = \{o.a_1a_2 \cdots a_n \mid a_1, a_2, \cdots, a_n \in \{0, 1\} \wedge a_n \neq 0\}$ halle el número de elementos de B_n y pruebe que $\bigcup_{n\in\mathbb{N}} B_n = B$ es numerable.

   (c) Transforme el resultado anterior para demostrar que el conjunto de todas las sucesiones finitas de ceros y unos es numerable.

7. Demuestre que si A es infinito y $B = \{b_0, b_1, b_2, \cdots\}$ es un subconjunto numerable de A y $A-B$ es aún infinito, entonces $(A-B) \approx A$. Ayuda: Tome en $A - B$ un subconjunto numerable $C = \{c_0, c_1, c_2 \cdots\}$ y establezca una biyección entre

$$A = ((A - B) - C) \cup C \cup B \quad \text{y} \quad A - B = ((A - B) - C) \cup C.$$

8. Sea A un conjunto numerable; si n es un número natural cualquiera, demuestre que la colección $\mathcal{P}_n(A)$ de los subconjuntos de A con a lo más n elementos, es numerable. Use este resultado para probar que la colección $\mathcal{P}_F(A)$ de todos los subconjuntos finitos de A es aún numerable. Ayuda: Pruebe que $A^n \succeq \mathcal{P}_n(A)$ hallando una función de A^n sobre $\mathcal{P}_n(A)$.

9. Sea A un conjunto contable; es costumbre notar por A^* al conjunto de todas las sucesiones finitas de elementos de A. Cuando una sucesión finita $a_1, a_2, \ldots, a_n$ se escribe solamente yuxtaponiendo de izquierda a derecha sus elementos $a_1 a_2 \cdots a_n$, se dice que es una *palabra* o una *expresión generada por el alfabeto* A; en este caso A^* se llama el conjunto de palabras o expresiones generadas por el alfabeto A. Pruebe que A^* es contable y que si A tiene uno o más elementos, A^* es numerable.

   Ayuda: Identifique $a_1 a_2 \cdots a_n$ con $(a_1, a_2, \cdots, a_n)$; así A^* se identifica con $\bigcup_{n=1}^{\infty} A^n$.

6.4 CONJUNTOS NO CONTABLES

El infinito como un ente existente, surge en los ámbitos filosófico y teológico; cuando se afirma que Dios es un ser infinitamente bueno, sabio y poderoso. *el infinito* es el grado en el cual Dios posee estas cualidades. Implícitamente se está asumiendo que *el* infinito es único; esta concepción de un infinito único se mantuvo durante mucho tiempo y llevó a quienes pretendieron analizar y aritmetizar dicho concepto (por ejemplo al sacerdote católico y matemático Bernardo Bolzano (1781-1848)) a contradicciones, las cuales junto con otras propiedades consideradas también paradójicas (como el que un conjunto infinito pueda ser equipotente con subconjuntos propios, contradiciendo la famosa noción común de Euclides "El todo es mayor que las partes"), se combinaron para retrasar la exploración sistemática del infinito.

Fue finalmente George Cantor quien entre 1873 y 1897 trató el infinito como una generalización del concepto de número, desarrolló alrededor de él toda una rama de la Matemática y lo introdujo no sólo en los otros campos matemáticos sino en las ciencias y en la misma filosofía (ver p. ej. [2]). Él descubrió y probó el teorema siguiente, donde se pone de presente que existe una pluralidad de infinitos.

TEOREMA 9. Teorema de Cantor: $A \prec \mathcal{P}(A)$.

Demostración. Puesto que la función $A \to \mathcal{P}(A)$ dada por $x \mapsto \{x\}$ es claramente inyectiva, se sigue que $A \preceq \mathcal{P}(A)$. La parte realmente interesante de la prueba consiste en demostrar que nunca se puede tener una función sobreyectiva de A en $\mathcal{P}(A)$ (y por consiguiente nunca se conseguirá una biyección de A en $\mathcal{P}(A)$). Lo hacemos por contradicción: Supongamos que exista una función $f : A \to \mathcal{P}(A)$ sobreyectiva; para cada x de A, siendo $f(x)$ un subconjunto de A, es posible que x sea elemento de su conjunto imagen $f(x)$; llamemos B al subconjunto de A formado por aquellos de sus elementos que no poseen esta propiedad, es decir, $B = \{x \in A \mid x \notin f(x)\}$. Siendo $B \in \mathcal{P}(A)$ y f sobreyectiva, existe al menos un elemento b de A tal que $f(b) = B$.

Pero: ¿ pertenece b a $f(b)$?.

Si $b \in f(b)$, entonces $b \in B$, luego b deberá cumplir la condición que define B, es decir $b \notin f(b)$. Si $b \notin f(b)$, entonces b cumple la propiedad que poseen los elementos de B, de modo que $b \in B$, y siendo $B = f(b)$, se obtiene $b \in f(b)$.

En resumen $b \in f(b) \longleftrightarrow \neg(b \in f(b))$, lo cual es una contradicción; como ésta proviene de suponer que f es sobreyectiva, se concluye que no existen sobreyecciones de A en $\mathcal{P}(A)$, quedando demostrado el teorema. □

Nótese que éste es en esencia el mismo argumento usado por Russell en su famosa paradoja, pero haciendo justicia a Cantor debemos recordar que su resultado antecedió varios años a la paradoja de Russell. Hoy en día las investigaciones históricas llevan a concluir que Russell concibió su paradoja a partir de este trabajo de Cantor.

Si A es infinito, también lo son $\mathcal{P}(A)$, $\mathcal{P}(\mathcal{P}(A))$, etc., existiendo toda una sucesión infinita de conjuntos infinitos no equipotentes:

$$A < \mathcal{P}(A) < \mathcal{P}(\mathcal{P}(A)) < \mathcal{P}(\mathcal{P}(\mathcal{P}(A))) < \cdots$$

Si definimos inductivamente

$$\mathcal{P}^0(A) = A \quad \mathcal{P}^{n+1}(A) = \mathcal{P}(\mathcal{P}^n(A)) \quad ,$$

entonces la sucesión anterior se transforma en

$$A < \mathcal{P}(A) < \mathcal{P}^2(A) < \mathcal{P}^3(A) < \cdots$$

Sea $L = \bigcup_{n\in\mathbb{N}} \mathcal{P}^n(A)$; claramente para todo n

$$\mathcal{P}^n(A) < \mathcal{P}^{n+1}(A) \subseteq L$$

y por la proposición 5,

$$(\forall n)(\mathcal{P}^n(A) < L)$$

pudiéndose alargar la sucesión

$$A < \mathcal{P}(A) < \mathcal{P}^2(A) < \cdots < L < \mathcal{P}(L) < \mathcal{P}^2(L) < \cdots$$

y el proceso puede repetirse cuantas veces se quiera. Si $A = \mathbb{N}$, todos los conjuntos anteriores serán infinitos, poniéndose de presente que hay al menos tantos tamaños de conjuntos infinitos como de números naturales.

A continuación estableceremos una relación importante y útil entre $\mathcal{P}(A)$ y el conjunto de las funciones de A en $\{0,1\}$:

Tomemos un conjunto A cualquiera y considerémoslo fijo en adelante; a cada subconjunto B de A se le puede hacer corresponder de manera unívoca la función $\lambda_B : A \to \{0,1\}$ tal que $\lambda_B(x) = 1$ si $x \in B$ y $\lambda_B(x) = 0$ si $x \notin B$. Se le acostumbra llamar la *función característica* de B (con respecto a A).

Si designamos por $\mathfrak{F}(A)$ al conjunto de todas las funciones de A en $\{0,1\}$, tenemos la siguiente:

PROPOSICIÓN 16. $\mathcal{P}(A) \approx \mathfrak{F}(A)$.

Demostración. Sea $F : \mathcal{P}(A) \to \mathfrak{F}(A)$ la función que a cada subconjunto B de A le asigna su correspondiente función característica; en otras palabras, $F(B) = \lambda_B$, claramente está bien definida porque $\lambda_B \in \mathfrak{F}(A)$.

a) F es inyectiva: Sean $B \neq C$ elementos de $\mathcal{P}(A)$; existe entonces un elemento x de B que no está en C o un y en C

que no está en B; en el primer caso $\lambda_B(x) = 1$ y $\lambda_C(x) = 0$; en el segundo $\lambda_B(y) = 0$ y $\lambda_C(y) = 1$, luego en cualquier caso $\lambda_B \neq \lambda_C$.

b) F es sobreyectiva: Si $f \in \mathfrak{F}(A)$, entonces f es una función de A en $\{0,1\}$; sea $B = \{x \in A \mid f(x) = 1\}$; claramente $B \in \mathcal{P}(A)$ y $f = \lambda_B = F(B)$, luego toda función de A en $\{0,1\}$ es una función característica de algún subconjunto de A, quedando demostrado.

□

Es costumbre usar la notación X^Y para designar al conjunto de todas las funciones del conjunto Y en el conjunto X (el motivo de tal notación se halla en el ejercicio 7 de la sección 4 del Cap. IV). Con dicha notación la proposición 16 toma la forma $\mathcal{P}(A) \approx \{0,1\}^A = 2^A$.

En particular si $A = \mathbb{N}$, $\mathcal{P}(\mathbb{N}) \approx \{0,1\}^{\mathbb{N}}$. Pero este último se identifica con el conjunto S de todas las sucesiones formadas con ceros y unos (ver Ejercicio 4 de la sección 3 del Cap. IV).

Según el ejercicio 6 de la sección anterior, el conjunto S_F de las sucesiones *finitas* de ceros y unos es numerable; pero S_F es equipotente con el conjunto S_0 de las sucesiones infinitas de ceros y unos que son periódicas de período cero, la biyección natural sería

$$a_0, a_1, a_2, \ldots, a_n \to a_0, a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots$$

Siendo $S \approx \mathcal{P}(\mathbb{N})$ y S_0 numerable, se sigue que $S - S_0$ es infinito (¡ no numerable!), luego por el ejercicio 7 de la sección anterior, $(S - S_0) \approx S$

Pero la función $f : S - S_0 \to]0,1] = \{x \in \mathbb{R} \mid 0 < x \leq 1\}$ definida por $f(a_0, a_1, a_2, \ldots) = 0.a_0a_1a_2\ldots$ es una biyección, ya que todo real de $]0,1]$ posee un único desarrollo binario no terminado en ceros (ver ejercicio 11c, sección 3 del Cap. V), es decir con forma de sucesión perteneciente a $S - S_0$.

Resumiendo:

TEOREMA 10. *El intervalo* $]0,1]$ *no es contable ya que*

$$]0,1] \approx \mathcal{P}(\mathbb{N}) \quad .$$

Existe otra forma de probar que $]0,1]$ no es numerable; vale la pena desarrollarla debido a que la técnica usada es muy fructífera en la matemática; también se debe a George Cantor.

Consiste en demostrar que no existe una función $f : \mathbb{N} \to]0,1]$ sobreyectiva, o lo que es igual, que nunca es posible disponer los reales de $]0,1]$ en forma de sucesión. La prueba se hace por contradicción. Supongamos que $]0,1] = \{a_0, a_1, a_2, \cdots\}$, se ha numerado biyectivamente; expresemos cada uno de los a_n como decimal infinito no terminado en ceros (ver ejercicio 10 de la sección 3 del Cap. V) para que su desarrollo sea único.

$$\begin{aligned} a_0 &= 0.a_{00}\, a_{01}\, a_{02}\, a_{03} \ldots \\ a_1 &= 0.a_{10}\, a_{11}\, a_{12}\, a_{13} \ldots \\ a_2 &= 0.a_{20}\, a_{21}\, a_{22}\, a_{02} \ldots \\ a_3 &= 0.a_{30}\, a_{31}\, a_{32}\, a_{33} \ldots \\ &\vdots \qquad\quad \vdots \end{aligned}$$

Formemos el decimal $b = 0.b_0 b_1 b_2 b_3 \ldots$ en la forma siguiente: $0 \neq b_0 \neq a_{00}$; $0 \neq b_1 \neq a_{11}$; $0 \neq b_2 \neq a_{22}$; en general $0 \neq b_n \neq a_{nn}$.

Evidentemente $b \in]0,1]$, ninguna cifra de b es cero y b es diferente de todos los a_n ya que de a_0 se diferencia al menos en su primera cifra, de a_1 se diferencia al menos en su segunda cifra, ..., y en general de a_n se diferencia al menos en su $n+1$ cifra. Se obtiene así una contradicción por estar b en $]0,1]$ y no ser de los de la lista precedente.

Si se trata de eliminar la aparente ambigüedad presentada en la construcción del número b, el método se puede cambiar ligeramente definiendo $b_n = 1$ si $a_{nn} \neq 1$ y $b_n = 2$ si $a_{nn} = 1$, obteniéndose b unívocamente.

El argumento anteriormente dado puede verse como la prueba de que ninguna lista numerable (o sucesión) puede incluir todos los reales de $]0,1]$; así como se formó b, se pueden también formar muchos otros (en realidad una cantidad infinita no contable), no pertenecientes a la sucesión, ya que para cada una de las cifras de b se tiene ocho posibilidades de elección.

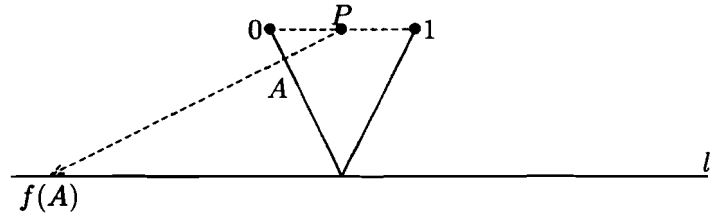
La técnica usada en la demostración se llama *"el método diagonal de Cantor"*.

De manera semejante a como se probó el corolario 3 del anterior teorema 2, también se puede demostrar que

$$]0,1] \approx]0,1[= \{x \in \mathbb{R} \mid 0 < x < 1\} \quad .$$

Ya sea utilizando la geometría euclidiana o algunas funciones reales conocidas, se puede probar fácilmente que $]0,1[\approx \mathbb{R}$.

Por ejemplo si "doblamos" por la mitad el intervalo $]0,1[$ y lo colocamos como en la figura,



de tal manera que el segmento que une a 0 con 1 sea paralelo con la recta l y P sea el punto medio de dicho segmento, se obtiene una biyección con solo asignar a cada punto A del segmento $]0,1[$ el punto $f(A)$ de la intersección de la recta $\overleftrightarrow{PA}$ con la recta l. Dejamos al lector que llene los detalles de la prueba de la biyectividad.

Resumiendo en un renglón los resultados anteriores,

$$\mathbb{R} \approx]0,1[\approx \{0,1\}^{\mathbb{N}} = 2^{\mathbb{N}} \approx \mathcal{P}(\mathbb{N})$$

y por el teorema de Cantor, $\mathbb{R} \succ \mathbb{N}$.

El mismo Cantor trató de contestar, sin lograrlo nunca, la pregunta siguiente: ¿Existe algún subconjunto A de $\mathbb{R}$ tal que $\mathbb{N} \prec A \prec \mathbb{R}$? o sea tal que $\mathbb{N} \prec A \prec 2^{\mathbb{N}}$?

Debido a que en la matemática clásica nunca se ha hallado un conjunto con tales características, Cantor *conjeturó* en 1878 que la respuesta debería ser *no*. A esta conjetura

$$\textit{No existe } A \textit{ tal que } \quad \mathbb{N} \prec A \prec 2^{\mathbb{N}}$$

se le ha llamado *la hipótesis del continuo*, debido a que ella equivale a que "todo subconjunto de $\mathbb{R}$ que no es contable, es equipotente con $\mathbb{R}$", o sea que "posee la potencia del continuo", es decir, que su cardinal es C, el cardinal del continuo (ver la proposición que sigue).

Una conjetura que generaliza la anterior, es la llamada *hipótesis generalizada del continuo*:

$$\text{Para todo } B \text{ infinito, no existe } A \text{ tal que } \quad B \prec A \prec 2^B \quad .$$

En 1938, Kurt Gödel demostró que si ella se agrega como un axioma más a la teoría de conjuntos, la nueva teoría así enriquecida también es consistente, siempre y cuando la antigua teoría sea consistente.

Tan sólo en 1963 se dilucidó el problema en el cual Cantor había fallado. El matemático americano Paul Cohen probó que dicha conjetura es independiente de los demás axiomas de la teoría de conjuntos (ver [3]).

La hipótesis del continuo viene así a tomar un carácter similar al famoso quinto postulado (de las paralelas) de Euclides con respecto a los demás axiomas.

El siguiente resultado también fruto de la genialidad de Cantor, pone de presente que hay tantos puntos en todo el plano como en una sola de sus rectas.

PROPOSICIÓN 17. $\mathbb{R} \times \mathbb{R} \approx \mathbb{R}$.

Demostración. Como $\mathbb{R} \approx]0,1]$, es suficiente probar que $]0,1] \times]0,1] \approx]0,1]$. Si $(x,y) \in]0,1] \times]0,1]$, expresemos tanto a x como a y en su expansión decimal (excluyendo terminaciones en ceros) y definamos

$$\begin{aligned} f(x,y) &= f(0.x_0x_1x_2\ldots, 0.y_0y_1y_2\ldots) \\ &= 0.x_0y_0x_1y_1x_2y_2\ldots \end{aligned}$$

Es realmente sencillo demostrar que tal función es inyectiva, de modo que $(]0,1] \times]0,1]) \preceq]0,1]$.

Como $g :]0,1] \to]0,1] \times]0,1]$ definida por $g(x) = (x,1)$ es inyectiva, también $]0,1] \preceq (]0,1] \times]0,1])$ y el resultado se sigue por el teorema de Cantor-Bernstein. □

COROLARIO 6. $\mathbb{R}^n \approx \mathbb{R}$, *cualquiera sea n natural no nulo.*

Demostración. Por inducción sobre n; para $n = 1$ es trivial; si $\mathbb{R}^n \approx \mathbb{R}$, entonces $\mathbb{R}^{n+1} = \mathbb{R}^n \times \mathbb{R} \approx \mathbb{R} \times \mathbb{R}$ por la hipótesis de inducción y este último producto es equipotente con $\mathbb{R}$ según la proposición 17. □

Ejercicios

1. Pruebe, construyendo explícitamente una biyección, que si A es un conjunto infinito y B es cualquier conjunto contable, entonces siempre $A \cup B \approx A$.

2. (a) Use el ejercicio 3 de la sección 1 para demostrar que $]0,1] \approx]0,1[$ y que $[0,1] \approx]0,1]$.

   (b) Pruebe las dos equipotencias de la parte (a) dando explícitamente las biyecciones correspondientes. Muestre además que $]0,1] \approx [0,1[$.

3. Usando la fórmula para sumar una progresión geométrica, compruebe que $1 = 0.1111\ldots$ y que $0.011000\cdots = 0.010111\ldots$ en el sistema binario; análogamente pruebe que $1 = 0.9999\ldots$ en el sistema decimal.

4. Si $a < b$ son reales cualesquiera, halle una biyección $f : [a,b] \to [0,1]$ de tipo polinomial de grado 1. Represente $[a,b]$ y $[0,1]$ por segmentos perpendiculares y halle una forma geométrica de establecer una biyección entre ellos. Se prueba así que dos segmentos cualesquiera, por pequeño que sea el uno y por grande que sea el otro, son equipotentes.

5. Haga ver que la técnica consistente en usar funciones características para determinar los subconjuntos de un conjunto A, si A es finito se transforma en un método directo para calcular el número de sus subconjuntos.

6. Sin usar el teorema 8 (teorema de Cantor), demuestre que el conjunto F de todas las funciones de $\mathbb{R}$ en $\mathbb{R}$ domina estrictamente a $\mathbb{R}$.

   Ayuda:

   (a) Para ver que $\mathbb{R} \preceq F$, considere el conjunto de las funciones constantes.

   (b) Para ver que $\neg(\mathbb{R} \approx F)$, suponga que $u : \mathbb{R} \to F$ es una biyección, entonces para cada función de F existe un único t del cual es imagen y podemos sin ambigüedad designarla por $f_t (= u(t))$. Use el método diagonal de Cantor para construir una función $g : \mathbb{R} \to \mathbb{R}$ diferente de todas las f_t (se debe diferenciar de la t-ésima función f_t precisamente en su valor en el punto t).

7. Demuestre que $\mathbb{N} \times \mathbb{R} \approx \mathbb{R}$. Ayuda: Pruebe que $\{n\} \times]0,1] \approx]n, n+1]$ y muestre que $\mathbb{N} \times]0,1] \approx \{x \in \mathbb{R} \mid 0 < x\} \approx \mathbb{R}$, o también compare $\mathbb{N} \times \mathbb{R}$ con $\{0\} \times \mathbb{R}$ y $\mathbb{R} \times \mathbb{R}$ y use el teorema de Cantor-Bernstein.

8. Demuestre que la función f de la proposición 17, no es sobreyectiva.

6.5 NÚMEROS CARDINALES

¿Qué es el *número de elementos* de un conjunto?

Ya nos habíamos hecho esta misma pregunta con respecto a los conjuntos finitos y en parte los números naturales fueron construidos para responderla: Para un conjunto finito, su número de elementos es cierto natural único y éste es el mismo para todos los conjuntos equipotentes con él, es decir,

$$\#(A) = \#(B) \Leftrightarrow A \approx B \quad .$$

Deseamos extender estas ideas para conjuntos infinitos, pero ya se vió que aun para los mismos conjuntos finitos falla la definición "natural" propuesta por Frege, $\#(A) = \{X \mid X \approx A\}$ debido a que éste no es un conjunto formado lícitamente puesto que no cumple las exigencias hechas dentro de nuestra teoría axiomática.

Para definir el número de elementos de manera similar a como se hizo con los conjuntos finitos, necesitamos antes definir los análogos de los números naturales; estos son los números ordinales, para los cuales se conserva tanto la buena ordenación como el concepto de sucesor. Finalmente se define cardinal (es decir el número de elementos) de un conjunto como un ordinal especial. Aplazamos esta construcción para más adelante cuando se tengan otros conocimientos auxiliares y por ahora nos salimos un poco por la tangente.

Vamos a considerar entonces el concepto *número de elementos* o *cardinal* como primitivo; esto significa que en vez de definirlo explícitamente en función de los demas terminos técnicos de la Teoría de Conjuntos lo haremos de una manera implícita, o sea que damos su significado a través de la forma como usamos este término en ciertos contextos. Así hemos aprendido el significado de muchas palabras de nuestro lenguaje cotidiano, sin necesidad de consultar el diccionario.

Queriendo generalizar la situación del caso finito y de acuerdo con nuestros conocimientos y nuestra bien formada intuición, es suficiente dar un solo axioma para caracterizar el concepto de cardinal.

Se sobrentiende que si A es cualquier conjunto (finito o infinito) su cardinal, notado $\text{Card}(A)$ o $\#(A)$, es también un conjunto, ya que como se dijo al comienzo, en nuestra teoría solo consideramos conjuntos.

Axioma de Cardinalidad.

Para cada conjunto A existe un conjunto notado $\text{Card}(A)$ tal que

(C1) $A \approx \text{Card}(A)$ y

(C2) $A \approx B$ si y sólo si $\text{Card}(A)=\text{Card}(B)$.

DEFINICIÓN 5. *Un conjunto α se llamará un* número cardinal *si y sólo si existe un conjunto A tal que $\alpha = \text{Card}(A)$.*

Sean α, β cardinales; supongamos que $\alpha = \#(A)$ y $\beta = \#(B)$ y que $A \preceq B$; si A', B' también son conjuntos tales que $\alpha = \#(A')$ y $\beta = \#(B')$, entonces por el axioma de cardinalidad $A \approx A'$ y $B \approx B'$; la proposición 2 implica que $A' \preceq B'$, o sea que la relación "$\preceq$" se conserva al cambiar los conjuntos por otros equipotentes.

Es entonces correcta la siguiente:

DEFINICIÓN 6. *Sean α, β cardinales tales que $\alpha = \#(A)$ y $\beta = \#(B)$*

$$\alpha \leq \beta \quad \text{significa} \quad A \preceq B \; .$$

Se deduce que $A \preceq B \leftrightarrow \#(A) \leq \#(B)$.

PROPOSICIÓN 18. *Sean α, β y γ cardinales cualesquiera; se tiene que*

i) $\alpha \leq \alpha$.

ii) $\alpha \leq \beta \wedge \beta \leq \gamma \rightarrow \alpha \leq \gamma$.

iii) $\alpha \leq \beta \wedge \beta \leq \alpha \rightarrow \alpha = \beta$.

Demostración. Las propiedades i) y ii) se deducen de sus correspondientes de la relación $\preceq$ y la iii) no es otra cosa, después del axioma de cardinalidad, que el teorema de Cantor-Bernstein. □

DEFINICIÓN 7. *Sean α, β cardinales cualesquiera; $\alpha < \beta$ significará $\alpha \leq \beta$ y $\neg(\alpha = \beta)$.*

PROPOSICIÓN 19. $A \prec B \longleftrightarrow \#(A) < \#(B)$.

Demostración. Es evidente de las definiciones 1, 6 y 7. □

Combinando este resultado con la proposición 4, se obtiene que la relación "$\alpha < \beta$" entre cardinales es independiente de los conjuntos A y B tales que $\alpha = \#(A)$ y $\beta = \#(B)$, de manera que la anterior proposición se puede modificar así:

PROPOSICIÓN 20. *Sean α, β tales que $\alpha = \#(A)$ y $\beta = \#(B)$; entonces $\alpha < \beta$ si y sólo si $A \prec B$.*

La proposición 5 se transforma en:

PROPOSICIÓN 21. *Si α, β, γ son cardinales tales que $(\alpha \leq \beta) \wedge (\beta \leq \gamma)$ y una de las dos desigualdades es estricta, entonces $\alpha < \gamma$.*

En el ejercicio 8 de la sección 4 del Cap. IV se definieron adición y multiplicación de cardinales y se pidió demostrar algunas de sus propiedades fundamentales. Si el lector realizó este ejercicio, puede limitarse a leer de corrido lo que sigue:

PROPOSICIÓN 22. *Si α, β son cardinales, existen conjuntos A y B tales que $\alpha = \#(A)$, $\beta = \#(B)$ y $A \cap B = \emptyset$.*

Demostración. De la definición 5, siempre existen conjuntos A' y B' tales que $\alpha = \#(A')$ y $\beta = \#(B')$; Sean $A = A' \times \{\emptyset\}$ y $B = B' \times \{\{\emptyset\}\}$. Evidentemente $A \approx A'$ y $B \approx B'$ y $A \cap B = \emptyset$, luego por el axioma de cardinalidad, $\alpha = \#(A)$ y $\beta = \#(B)$. □

PROPOSICIÓN 23. *Si $A \cap B = \emptyset$ y $A' \cap B' = \emptyset$ y $A \approx A'$ y $B \approx B'$, entonces $A \cup B \approx A' \cup B'$.*

Demostración. Sean $f : A \to A'$ y $g : B \to B'$ las biyecciones que establecen las equipotencias; debido a que tanto sus dominios como sus recorridos son disyuntos, el corolario 2 del teorema 10 del Cap. II establece que $f \cup g$ es una biyección de $A \cup B$ en $A' \cup B'$. □

DEFINICIÓN 8. *Si α, β son cardinales, definimos $\alpha + \beta$ como el cardinal de $A \cup B$, done A, B son conjuntos tales que*

$$\alpha = \#(A), \quad \beta = \#(B) \quad \text{y} \quad A \cap B = \emptyset \quad .$$

Esta definición es correcta ya que según la proposición 19 siempre existen conjuntos que llenan las condiciones exigidas, y la proposición 23 muestra que $\alpha + \beta$ no depende de los conjuntos escogidos.

TEOREMA 11. *La adición de números cardinales es asociativa, conmutativa y modulativa.*

Demostración. Dichas propiedades son consecuencias inmediatas de las correspondientes de la unión de conjuntos: $(A \cup B) \cup C = A \cup (B \cup C)$, $A \cup B = B \cup A$ y $A \cup \emptyset = A$. ($\#(\emptyset) = 0$ es el módulo).

Además dejamos como ejercicio probar que

$$\alpha \leq \beta \to \alpha + \gamma \leq \beta + \gamma \quad ,$$

o sea la *monotonía de la adición con respecto al* orden "$\leq$".

Debido a que los cardinales pueden ser infinitos, no es válida la propiedad cancelativa; por ejemplo si designamos por $\aleph_0$ al cardinal del conjunto de los números naturales y por C al cardinal del conjunto de los reales, se tiene que:

1. $\aleph_0 + n = \aleph_0$, cualquiera sea n natural.[4]
2. $\aleph_0 + \aleph_0 = \aleph_0$.
3. $C + C = C$.
4. $C + \aleph_0 = C$.

En realidad del ejercicio 1 de la sección anterior se deduce que $\alpha + n = \alpha$ cualquiera sea el cardinal infinito α.
Como $\aleph_0 = \#(\{n \in \mathbb{Z} \mid n < 0\}) = \#(\{n \in \mathbb{Z} \mid n \geq 0\})$, se deduce que $\aleph_0 + \aleph_0 = \#(\{n \in \mathbb{Z} \mid n < 0\} \cup \{n \in \mathbb{Z} \mid n \geq 0\}) = \#(\mathbb{Z}) = \aleph_0$.

La igualdad 3. se prueba por ejemplo así:

$$C + C = \#(]0,1]) + \#(]1,2]) = \#(]0,1] \cup]1,2]) = \#(]0,2]) = C \quad .$$

Usando la montonía, $C \leq C + \aleph_0 \leq C + C = C$ y la antisimetría de "$\leq$" implica $C + \aleph_0 = C$.

De manera análoga se procede con la multiplicación de cardinales: si α, β son cardinales, entonces existen conjuntos A, B tales que $\alpha = \#(A)$ y $\beta = \#(B)$; definimos $\alpha\beta$ como el cardinal de $A \times B$; el corolario 1 del teorema 10 del Cap. III muestra que ésta operación está bien definida; el ejercicio 8 de la sección 1 de este capítulo nos dice que es conmutativa y asociativa y el ejercicio 7 de la misma sección 1, que si $\alpha \leq \beta \wedge \gamma \leq \delta$ entonces $\alpha\gamma \leq \beta\delta$ (monotonía). Es claro además que $A \times \{\emptyset\} \approx A$, de modo que $\#(\{\emptyset\}) = 1$ es el módulo de la multiplicación. Como $A \times (B \cup C) = (A \times B) \cup (A \times C)$ y cuando $B \cap C = \emptyset$ se tiene que $(A \times B) \cap (A \times C) = \emptyset$, se deduce que para cardinales se cumple la distributividad de la multiplicación con respecto a la adición:

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma.$$

[4] Se supone, como en realidad se verá más tarde , que los naturales son los cardinales de los conjuntos finitos.

Otro resultado válido es $\alpha \cdot 0 = 0$, ya que $A \times \emptyset = \emptyset$; pero no se cumple la cancelativa del producto, ya que por ejemplo

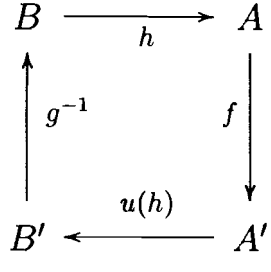
$$n \cdot C = C, \qquad \text{para } n \text{ natural mayor que cero.}$$
$$\aleph_0 \cdot C = C.$$
$$C \cdot C = C.$$

(Las tres se pueden deducir de $C = 1 \cdot C \leq n \cdot C \leq \aleph_0 \cdot C \leq C \cdot C = C$; la última igualdad es consecuencia de la proposición 17). □

Pasamos finalmente a tratar la exponenciación de cardinales; ya en la sección 3 se introdujo la notación X^Y para designar al conjunto de todas las funciones de Y en X; el motivo de tal notación está precisamente en que para conjuntos finitos se obtuvo el resultado $\#(X^Y) = (\#(X))^{(\#(Y))}$; lo único que se pretende es definir la exponenciación en el caso general de tal manera que esta igualdad se conserve y además se cumplan sus propiedades usuales.

PROPOSICIÓN 24. *Si $A \approx A'$ y $B \approx B'$, entonces $A^B \approx A'^{B'}$.*

Demostración. Sean $f : A \to A'$ y $g : B \to B'$ las biyecciones que establecen las equipotencias de la hipótesis; definimos una función $u : A^B \to A'^{B'}$ mediante $u(h) = f \circ h \circ g^{-1}$, como lo muestra el diagrama adjunto.



La función u es inyectiva ya que si $u(h) = u(h^*)$, o sea si $f \circ h \circ g^{-1} = f \circ h^* \circ g^{-1}$, entonces $f^{-1} \circ (f \circ h \circ g^{-1}) \circ g = f^{-1} \circ (f \circ h^* \circ g^{-1}) \circ g$ y efectuando operaciones, $h = h^*$; claramente u es sobreyectiva puesto que si $F \in A'^{B'}$, entonces $f^{-1} \circ F \circ g \in A^B$ y $u(f^{-1} \circ F \circ g) = F$. □

DEFINICIÓN 9. *Si α, β son cardinales, definimos α^β como $\#(A^B)$, donde A, B son tales que $\alpha = \#(A)$ y $\beta = \#(B)$.*

La definición es enteramente correcta ya que por la proposición anterior $\#(A^B) = \#(A'^{B'})$, es decir, no depende de los conjuntos elegidos.

TEOREMA 12. *Si α, β, γ son cardinales cualesquiera, se cumple que*

(i) $\gamma^\alpha \cdot \gamma^\beta = \gamma^{\alpha+\beta}$.

(ii) $(\alpha\beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$.

(iii) $(\alpha^\beta)^\gamma = \alpha^{(\beta \cdot \gamma)}$.

Demostración.

(i) Sean A, B, C conjuntos tales que $\alpha = \#(A)$, $\beta = \#(B)$ y $\gamma = \#(C)$ y $A \cap B = \emptyset$.

Es suficiente probar que $C^A \times C^B \approx C^{(A \cup B)}$.

Si $f \in C^{A \cup B}$, entonces $f : A \cup B \to C$; consideremos sus restricciones $f\restriction_A A :\to C$ y $f\restriction_B B :\to C$; la pareja ordenada de restricciones $(f\restriction_A, f\restriction_B)$ es un elemento de $C^A \times C^B$, luego $u(f) = (f\restriction_A, f\restriction_B)$ es una función de $C^{A \cup B}$ en $C^A \times C^B$; veamos que es una biyección: Si $f, g \in C^{A \cup B}$ y $f \neq g$, existe al menos un elemento x de $A \cup B$ tal que $f(x) \neq g(x)$;

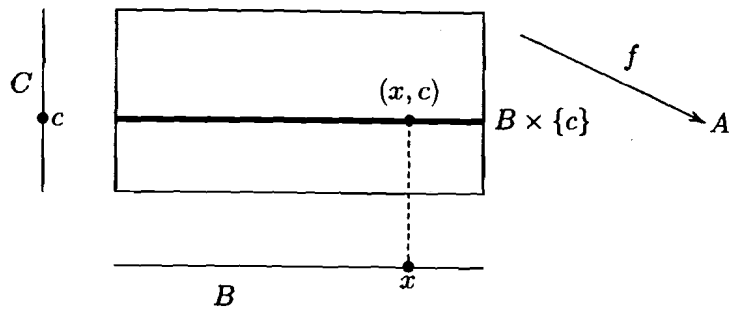
$$si \quad x \in A, \quad f\restriction_A(x) \neq g\restriction_A(x); \quad \text{si} \quad x \in B, \quad f\restriction_B(x) \neq g\restriction_B(x);$$

en cualquier caso, $(f\restriction_A, f\restriction_B) \neq (g\restriction_A, g\restriction_B)$, así que u es inyectiva. Si $(h_1, h_2) \in C^A \times C^B$, entonces $h_1 : A \to C$ y $h_2 : B \to C$ y siendo disyuntos los dominios entonces (teorema 6 Cap. IV) $f = h_1 \cup h_2$ es una función de $A \cup B$ en C y claramente $h_1 = f\restriction_A$ y $h_2 = f\restriction_B$, o sea que $u(f) = (h_1, h_2)$, luego u es sobreyectiva.

(ii) Sean A, B y C tales que $\alpha = \#(A)$, $\beta = \#(B)$ y $\gamma = \#(C)$; es suficiente probar que $(A \times B)^C \approx A^C \times B^C$.

Si $f \in (A \times B)^C$, entonces $f : C \to A \times B$, de modo que para todo $c \in C$, $f(c) = (a, b)$; sean $f_1(c) = a$ y $f_2(c) = b$; éstas son funciones de C en A la primera y de C en B la segunda (son las funciones componentes usuales). Dejamos al lector los detalles de la comprobación de la biyectividad de la función $f \mapsto (f_1, f_2)$.

(iii) Con la notación introducida en (ii), se debe demostrar precisamente que $(A^B)^C \approx A^{(B \times C)}$. Sea $f \in A^{B \times C}$, es decir $f : B \times C \to A$; para cada $c \in C$, definamos una función $f_c : B \to A$ tal que $f_c(x) = f(x, c)$ (o sea que $f_c = f\restriction_{B \times \{c\}}$).



Definimos una función $h_f : C \to A^B$ mediante $h_f(c) = f_c$; evidentemente $h_f \in (A^B)^C$. Veamos que la función $u(f) = h_f$ es una biyección: Si $f, g \in A^{B\times C}$ y $f \neq g$, existe al menos un punto (b, c) en $B \times C$ tal que $f(b, c) \neq g(b, c)$; entonces $f_c(b) \neq g_c(b)$, luego $f_c \neq g_c$; pero $h_f(c) = f_c$ y $h_g(c) = g_c$, de manera que $h_f(c) \neq h_g(c)$, es decir $h_f \neq h_g$, o sea que u es uno a uno.

Si $h : C \to A^B$, para cada c en C se tiene que $h(c)$ es una función de B en A; por lo tanto, definimos $F : B \times C \to A$ mediante $F(b, c) = h(c)(b)$.

La demostración queda completa probando que $u(F) = h_F = h$; cualesquiera sean $c \in C$ y $b \in B$ se tiene que $h_F(c)(b) = F_c(b) = F(b, c) = h(c)(b)$, o sea que para todo c, $h_F(c) = h(c)$, es decir $h_F = h$. □

Cansados después de probar el teorema anterior, dejamos como trabajo para el lector las demostraciones de los resultados siguientes.

PROPOSICIÓN 25.

a) $\alpha^0 = 1$, *cualquiera sea el cardinal* α *(observe que* $0^0 = 1$*).*

b) *Si* $\alpha \neq 0$, *entonces* $0^\alpha = 0$.

c) $\alpha^1 = \alpha$.

d) $\alpha^\beta = 0$ *si y sólo si* $\alpha = 0 \wedge \beta \neq 0$.

TEOREMA 13.

a) $\alpha \leq \beta \to \alpha^\gamma \leq \beta^\gamma$.

b) *Si* $d \neq 0 \wedge \alpha \leq \beta$, *entonces* $d^\alpha \leq d^\beta$.

Como consecuencia inmediata, tenemos el siguiente

TEOREMA 14.

a) $C^{\aleph_0} = C$.

b) $\aleph_0{}^{\aleph_0} = C$.

c) $2^C = (\aleph_0)^C = C^C$.

En términos de conjuntos, a) y b) dicen que el conjunto de todas las sucesiones de reales y el de todas las sucesiones de naturales, poseen el mismo cardinal que $\mathbb{R}$, es decir que el conjunto de todas las sucesiones formadas con ceros y unos solamente; c) dice que $\mathcal{P}(\mathbb{R})$ posee el mismo cardinal que el conjunto de todas las funciones de $\mathbb{R}$ en $\mathbb{R}$.

Demostración.

a) $C^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = C$.

b) $C = 2^{\aleph_0} \leq \aleph_0{}^{\aleph_0} \leq C^{\aleph_0} = C$.

c) $2^C \leq \aleph_0{}^C \leq C^C = (2^{\aleph_0})^C = 2^{\aleph_0 \cdot C} = 2^C$.

□

Ejercicios

1. Realice todas las demostraciones o partes de ellas que hemos dejado como trabajo para el lector.

2. ¿Es cierto o no que para cardinales cualesquiera si $\alpha < \beta$ entonces $\alpha + \gamma < \beta + \gamma$? Dé las razones de su respuesta.

3. Revise cuidadosamente todo el capítulo IV y diga cuáles de los resultados en él establecidos son consecuencia del teorema 2, al cual hemos llamado *teorema fundamental.*

4. Demuestre por inducción que si α es cualquier cardinal (finito o infinito), $n\alpha = \alpha + \alpha + \cdots + \alpha$ (n veces), y que si $n > 0$, $\alpha^n = \alpha \cdot \alpha \cdots \alpha$ (n veces).

5. Pruebe que para todo natural $n > 0$, $\aleph_0^n = \aleph_0$.

6.

a) Use el resultado anterior para demostrar que si A es numerable y n es un natural mayor que cero, la colección de las sucesiones finitas de longitud n de elementos de A, también es numerable.

b) Concluya que la colección de *todas* las sucesiones finitas de elementos de A también es numerable.

7. Demuestre que la coleción $\mathcal{P}_c(\mathbb{R})$ de todos los subconjuntos contables de $\mathbb{R}$ también tiene cardinal C. Ayuda: Pruebe que $\mathbb{R}^{\mathbb{N}} \succeq \mathcal{P}_c(\mathbb{R})$ hallando una función del primero *sobre* el segundo y luego use el resultado $C^{\aleph_0} = C$.

8. Dé contraejemplos adecuados para probar que ni la adición ni la multiplicación de cardinales son operaciones cancelativas.

9. Sea A un conjunto numerable; verifique que $A^A \subseteq \mathcal{P}(A \times A)$ y use este hecho para probar que $A^A \preceq \mathcal{P}(A)$.

   Muestre que $2^A \preceq A^A$ y concluya que $A^A \approx \mathcal{P}(A)$. Deduzca de este resultado que ${\aleph_0}^{\aleph_0} = 2^{\aleph_0}$.

10. Pruebe o refute que "el conjunto de todas las funciones inyectivas de A en A es equipotente con 2^A".

11. Si $(\alpha)_{i\in I}$ es una familia de números cardinales, pruebe que existe una familia de conjuntos $(A)_{i\in I}$ tal que

    (a) $(\forall i \in I)(\alpha_i = \#(A_i))$ y

    (b) $(\forall i, j \in I)(i \neq j \to A_i \cap A_j = \emptyset)$.

    Si $(B)_{i\in I}$ es otra familia de conjuntos que cumple a) y b), muestre que $\bigcup_{i\in I} A_i \approx \bigcup_{i\in I} B_i$.

    Si $(C)_{i\in I}$ cumple a), muestre que $\prod_{i\in I} A_i \approx \prod_{i\in I} C_i$.

12. En concordancia con el ejercicio anterior, es correcto definir suma y producto de una familia de cardinales en la forma:

$$\sum_{i\in I} \alpha_i \overset{\text{Def}}{=} \#\left(\bigcup_{i\in I} A_i\right).$$

$$\prod_{i\in I} \alpha_i \overset{\text{Def}}{=} \#\left(\prod_{i\in I} A_i\right) = \#\left(\prod_{i\in I} C_i\right).$$

(a) Halle

$$\sum_{n\in\mathbb{N}} n.$$

(b) Pruebe que si $(\forall n \in \mathbb{N})(\alpha_n = C = \#(\mathbb{R}))$, entonces

$$\sum_{n\in\mathbb{N}} \alpha_n = \aleph_0 C = C \quad \text{y que} \quad \prod_{n\in\mathbb{N}} \alpha_n = C^{\aleph_0} = C.$$

(c) Generalice los resultados anteriores, esto es, demuestre que el producto $\alpha\beta$ de dos cardinales puede obtenerse como una suma $\beta + \beta + \cdots$ de tantos sumandos iguales a β como α, y que β^α puede obtenerse como un producto de tantos factores iguales a β como α.

Ayuda: $A \times B = \bigcup_{a\in A}(\{a\} \times B) = \bigcup_{a\in A} B_a$ y los B_a son disyuntos dos a dos.

**

Capítulo 7

ELECCIÓN, CARDINALIDAD Y REGULARIDAD

En el presente capítulo veremos algunos enunciados del axioma de elección que involucran relaciones de orden; son los llamados principios maximales; a su vez los usaremos para obtener la comparabilidad de cardinales y el teorema de la buena ordenación. Además estudiaremos el axioma de regularidad y algunas de sus consecuencias sobre la estructura interna de los conjuntos.

7.1 ORDEN Y ELECCIÓN

Para comenzar, recordemos que si R es una relación de orden sobre un conjunto X y A es un subconjunto de X, $R \cap (A \times A)$ es una relación de orden sobre A y se dice que ésta es inducida por la primera; siempre que consideremos un subconjunto de un conjunto ordenado, lo supondremos provisto de su ordenación inducida.

Sea X un conjunto ordenado por $\preceq$; una $\preceq$-cadena de X (o simplemente una cadena cuando no haya lugar a confusión respecto del orden en consideración) es un subconjunto de X totalmente ordenado por la relación de orden inducida por $\preceq$.

Se dice que $a \in X$ es un elemento maximal de X (con respecto a $\preceq$) si $\neg(\exists y \in X)((a \preceq y) \wedge (a \neq y))$, es decir si a no es sucedido por ningún otro

elemento de X.

La proposición que sigue fue demostrada por K. Kuratowski en 1912, usando el axioma de elección; unos diez años más tarde, M. Zorn probó que ella a su vez implica el axioma de elección; debido a que fue la primera vez que alguien demostró la equivalencia de un principio maximal con el axioma de elección, hoy en día la iniciativa de N. Bourbaki se le llama "lema de Zorn".

LEMA DE ZORN. (LZ) *Si X es un conjunto ordenado por la relación $\preceq$, tal que toda $\preceq$-cadena de X es acotada superiormente en X, entonces X posee al menos un elemento maximal.*

La demostración de esta proposición es bastante laboriosa y no la daremos aquí; el lector interesado puede consultar [5] pág. 93 a 97.

Los principios maximales como el lema de Zorn, han reemplazado al mismo axioma de elección en muchas de sus aplicaciones en Algebra y Topología.

Para ilustrar la forma como se usa el lema de Zorn, probemos que éste implica al axioma de elección AE'.

Sea X un conjunto no vacío; una función de elección para X debe ser tal que $f(A) \in A$ para todo subconjunto A no vacío de X; la idea de la construcción de una función tal está en tomar una f_1 tal que su dominio sea un subconjunto de $\mathcal{P}(X)-\{\emptyset\}$ y que $f_1(A) \in A$ para todo A de su dominio, e ir extendiéndola poco a poco hasta que su dominio sea $\mathcal{P}(X) - \{\emptyset\}$. La función f_1 podría ser por ejemplo $\{(\{a\},a).(\{a,b\},b),(X,a)\}$, donde a,b están en X. Como para un conjunto X infinito el proceso sugerido no terminaría nunca, se procede en la forma siguiente:

Sea $\mathfrak{F}$ el conjunto de todas las funciones f que cumplen: $\mathcal{R}(f) \subseteq X$, $Dom(f) \subseteq (\mathcal{P}(X) - \{\emptyset\})$, y $(\forall A \in Dom\,(f))(f(A) \in A)$. Por el ejemplo dado se ve que $\mathfrak{F} \neq \emptyset$; ordenemos $\mathfrak{F}$ por contenencia, es decir $f \leq g$ significa $f \subseteq g$ (como conjuntos de parejas ordenadas que son) o lo que es lo mismo, g es una extensión de f.

Sea $\mathfrak{C}$ una cadena de $\mathfrak{F}$; como deseamos aplicar el lema de Zorn, debemos ver que $\mathfrak{C}$ es acotada superiormente, para lo cual una forma usual de hacerlo cuando el orden es la inclusión, consiste en ver simplemente que $\cup\mathfrak{C} \in \mathfrak{F}$ (ya que trivialmente $(\forall f \in \mathfrak{C})(f \subseteq \cup\mathfrak{C})$).

En efecto:

i) $\cup\mathfrak{C}$ es una función, ya que si $(a,b) \in \cup\mathfrak{C}$ y $(a,c) \in \cup\mathfrak{C}$, existen $f,g \in \mathfrak{C}$ tales que $(a,b) \in f$ y $(a,c) \in g$, pero siendo $\mathfrak{C}$ una cadena, $f \subseteq g$ ó $g \subseteq f$; en cualquier caso (a,b) y (a,c) están en una misma función lo cual implica $b = c$.

ii) $\mathcal{D}\,(\cup\mathfrak{C})=\mathcal{D}(\bigcup_{f\in\mathfrak{C}} f)=\bigcup_{f\in\mathfrak{C}} \mathcal{D}(f) \subseteq (\mathcal{P}(X) - \{\emptyset\})$ y por la propiedad análoga del recorrido se concluye $\mathcal{R}(\cup\mathfrak{C}) \subseteq X$.

iii) Si $A \in \mathcal{D}(\cup\mathfrak{C}) = \bigcup_{f\in\mathfrak{C}} \mathcal{D}(f)$, existe $f \in \mathfrak{C}$ tal que $A \in \mathcal{D}(f)$ y en consecuencia $f(A) \in A$, con lo cual termina la verificación ya que siendo $\cup\mathfrak{C}$ una extensión de f, también la imagen de A por $\cup\mathfrak{C}$ es $f(A)$.

Concluimos que $\cup\mathfrak{C} \in \mathfrak{F}$ y por consiguiente es una cota superior de $\mathfrak{C}$. Por el lema de Zorn existe entonces al menos una función g maximal en $\mathfrak{F}$; resta por demostrar $\mathcal{D}(g) = \mathcal{P}(X) - \{\emptyset\}$. Si existiese $B \in \mathcal{P}(X) - \{\emptyset\}$ tal que B no estuviese en $\mathcal{D}(g)$, como $B \neq \emptyset$, tomando $b \in B$ podríamos formar $h = g \cup \{(B,b)\}$, la cual estaría en $\mathfrak{F}$ y sería una extensión estricta de g, en contradicción con el hecho de ser g maximal.

En 1914 Hausdorff demostró los principios maximales que hoy en día llevan su nombre; a la postre son ligeras variantes del lema de Zorn:

Primer Principio maximal de Hausdorff (H1)
Todo conjunto ordenado posee al menos una cadena maximal.

Segundo Principio maximal de Hausdorff (H2)
Toda cadena de un conjunto ordenado está contenida en una cadena maximal.

Demostremos que estos dos principios son equivalentes al lema de Zorn:

1. El lema de Zorn implica H1
   Sea $\leq$ un orden para X y sea $\mathfrak{X}$ la colección de todas las $\leq$-cadenas de X; ordenemos $\mathfrak{X}$ por inclusión. Si $\mathfrak{C}$ es una cadena en $\mathfrak{X}$ (o sea $\subseteq$-cadena de $\leq$-cadenas), su unión $\bigcup_{A\in\mathfrak{C}} A$ resulta ser también una $\leq$-cadena de X, ya que si $x,y \in \bigcup_{A\in\mathfrak{C}} A$, existen $A,B \in \mathfrak{C}$ tales que $x \in A \wedge y \in B$; siendo $\mathfrak{C}$ una $\subseteq$-cadena, $A \subseteq B \vee B \subseteq A$ luego $x,y \in A$ ó $x,y \in B$; en cualquier caso x y y son comparables. De lo anterior se deduce que $\bigcup_{A\in\mathfrak{C}} A$ es una cota superior de $\mathfrak{C}$ y por el lema de Zorn aplicado a $\mathfrak{X}$ se concluye que éste posee un elemento maximal el cual es precisamente una $\leq$-cadena maximal de X.

2. H1 implica H2.
   Sea $\leq$ un orden para X (no vacío) y sea C una $\leq$-cadena de X ; sea θ_C la colección, ordenada por inclusión, de todas las $\leq$-cadenas de

X que contienen a C. Según H1, θ_C posee al menos una $\subseteq$-cadena maximal $\mathfrak{C}$; si $\hat{C} = \bigcup_{A\in\mathfrak{C}} A$, éste resulta ser una $\leq$-cadena maximal de X que contiene a la cadena C, como puede comprobarlo el lector.

3. **H2 implica L.Z**
   Sea X un conjunto no vacío ordenado por $\leq$ y tal que en él toda cadena es acotada superiormente. Sea a cualquier elemento de X; trivialmente el conjunto unitario $\{a\}$ es una $\leq$-cadena de X, de modo que por H2 deberá estar contenida en una $\leq$-cadena maximal C.

   Pero por hipótesis C está acotada superiormente; sea b cualquier cota superior de C; claramente $b \in C$ porque de lo contrario $C \cup \{b\}$ sería una cadena que contendría estrictamente a C y C no sería maximal; b es un elemento maximal de X porque si existiese $d \neq b$ tal que $b \leq d$, entonces $C \cup \{d\}$ sería una cadena que contendría estrictamente a C y así C no sería maximal. ⊡

Con esto hemos cerrado nuestra cadena de implicaciones.

Cambiando ligeramente de tema, recordemos que en el Cap. IV, sección 3 se probó el principio de inducción transfinita, el cual nos permite realizar por inducción demostraciones de propiedades relacionadas con elementos de los conjuntos bien ordenados. *¿Y si todo conjunto se pudiese ordenar bien?*

Esta conjetura parece a primera vista que va contra la intuición, ya que nuestra experiencia personal nos pone de presente lo difícil que es hallar un buen orden para un conjunto; por ejemplo para el conjunto $\mathbb{R}$ de los números reales nadie ha podido hallar un buen orden.

Sin embargo, E. Zermelo publicó en 1904 una demostración de la conjetura anterior; en ella además de los axiomas usuales de la tería de conjuntos, empleó el axioma de elección. No pudiéndose descubrir ningún error en la demostración de tan fuerte y poderoso resultado, muchos matemáticos optaron por atacar el axioma de elección, a pesar de que antes lo habían usado como una verdad prácticamente autoevidente. En 1909 el mismo Zermelo publicó una segunda prueba en la cual dio más participación a la lógica y menos a los conjuntos, pero sin poder suprimir claro está el uso del axioma de elección. El lector interesado puede leer en [4], pág. 84-86, la primera demostración efectuada por Zermelo del hoy llamado "teorema de la buena ordenación". Por razones didácticas no seguiremos el orden histórico y preferiremos probarlo usando el lema de Zorn; enunciémoslo con precisión:

TEOREMA 1. TEOREMA DE LA BUENA ORDENACIÓN
Todo conjunto puede ser bien ordenado, es decir, para cualquier conjunto X existe una relación de orden "$\leq$" tal que $(X, \leq)$ es bien ordenado .

Idea de la demostración: Si $X = \emptyset$, es evidente ya que $\emptyset$ es un buen orden para $\emptyset$.

Sea $X \neq \emptyset$; la estrategia de la prueba consiste en tomar un subconjunto pequeño de X, definirle un buen orden, e ir agregándole elementos pero en forma tal que no se cambie el orden que ya poseía el conjunto pequeño; téoricamente el proceso se continúa hasta ordenar bien a todo X. Para ello lo mejor es ir colocando cada elemento nuevo *después* de todos los existentes previamente. Por ejemplo, como $X \neq \emptyset$, sea $a \in X$; el conjunto $\{a\}$ es bien ordenado por $\{(a,a)\}$; sea $b \in X - \{a\}$; el conjunto $\{a,b\}$ es bien ordenado por $\{(a,a),(b,b),(a,b)\}$, es decir, $a < b$. Si $X - \{a,b\} = \emptyset$, el proceso termina; en caso contrario sea $c \in X - \{a,b\}$ y consideremos $\{a,b,c\}$ bien ordenado mediante $a < b < c$, es decir, $\{(a,a),(b,b),(c,c),(a,b),(a,c),(b,c)\}$. Si $X - \{a,b,c\} = \emptyset$ el proceso termina y si no sea $d \in X - \{a,b,c\}$ y consideremos $\{a,b,c,d\}$ bien ordenado mediante $a < b < c < d$. Observemos que $\{a\} \subset \{a,b\} \subset \{a,b,c\} \subset \{a,b,c,d\}$ y que el orden de cada conjunto es una extensión del orden del anterior, pero colocando cada elemento nuevo depués de todos los ya existentes, es decir

$$\{a\} = \sigma(b) \quad ; \quad \{a,b\} = \sigma(c) \quad ; \quad \{a,b,c\} = \sigma(d).$$

Decimos que cada nuevo conjunto ordenado es una *continuación* del anterior. Con más precisión:

DEFINICIÓN 1. *Un conjunto bien ordenado $(B, \leq)$ se llama una continuación de un conjunto bien ordenado A si:*

a) $B \supseteq A$,

b) El orden de A es el inducido por el de B y

c) Existe a en B tal que $A = \sigma(a) = \{x \in B \mid x < a\}$.

Más precisamente, un conjunto bien ordenado $(B, \leq)$ es una continuación de otro bien ordenado (A, R) si $R = (A \times A) \cap \leq$ y A es un segmento inicial de B, es decir $(\exists a \in B)(A = \{x \in B \mid x < a\})$. Debemos notar que "es una continuación de" es una relación de orden estricto para cualquier colección de conjuntos bien ordenados.

LEMA 1. *Si una familia $(X_i, \leq_i)_{i\in I}$ de conjuntos bien ordenados es una cadena con respecto a la continuación, entonces $(\bigcup_{i\in I} X_i, \bigcup_{i\in I} \leq_i)$ también es un conjunto bien ordenado y además es una continuación de cualquiera de los conjuntos dados que sea diferente de $\bigcup_{i\in I} X_i$.*

Demostración. Por el ejercicio 17 de la sección 7 del Cap. III, se ve que $\bigcup_{i\in I} \leq_i$ es un orden total sobre $X = \bigcup_{i\in I} X_i$ de manera que basta probar que es un buen orden. Sea $A \subseteq X$, $A \neq \emptyset$; existe entonces un X_i tal que $A \cap X_i \neq \emptyset$; $A \cap X_i$ tiene primer elemento, digamos a_0, por ser un subconjunto no vacío del conjunto bien ordenado X_i; veamos que a_0 es el primer elemento de A: Sea b cualquier otro elemento de A; en particular $b \in \bigcup_{i\in I} X_i$, de modo que $b \in X_j$, para algún j en I; si $X_i = X_j$, $b \in A \cap X_i$ y a_0 precede a b; si X_i es una continuación de X_j, $b \in A \cap X_j \subseteq A \cap X_i$ y así es precedida por a_0; si X_j es una continuación de X_i, existe d en X_j tal que $X_i = \{x \in X_j \mid x <_i d\}$;

i) Si $b <_i d$, entonces $b \in X_i$ y así $b \in A \cap X_i$, de modo que a_0 precede a b.

ii) Si $d <_i b$, como $a_0 \in X_i = \sigma(d)$ se tiene que $a_0 <_i d$ y por transitividad $a_0 <_i b$.

Se concluye que a_0 es el primer elemento de A. Claramente X es una continuación de cada uno de los X_i diferentes de X ya que si u es el primer elemento de $X - X_i$, entonces $X_i = \sigma(u)$.

Procedamos ahora *a demostrar el teorema de la buena ordenación*: Como el proceso que habíamos iniciado antes de ir alargando los subconjuntos y sus buenos órdenes, no termina manualmente si X es infinito, debemos aplicar el lema de Zorn:

Sea $\mathbb{B}$ la colección de todos los subconjuntos bien ordenados de X y ordenemos a $\mathbb{B}$ por continuación. Si $\mathfrak{C}$ es una cadena en $\mathbb{B}$ para la continuación, según el lema 1 anterior, su unión también está en $\mathbb{B}$ y es una cota superior de $\mathfrak{C}$, luego por el lema de Zorn existe un subconjunto M de X bien ordenado maximal. Afirmamos que $M = X$, ya que si existiese $a \in (M - X)$, entonces $M \cup \{a\}$ sería una continuación de M con sólo extender la ordenación de M colocando al elemento a después de todos los de M (si (M, R) es bien ordenado y $\overline{R} = R \cup \{(a,a)\} \cup \{(x,a) \mid x \in M\}$, entonces $(M \cup \{a\}, \overline{R})$ es bien ordenado). □

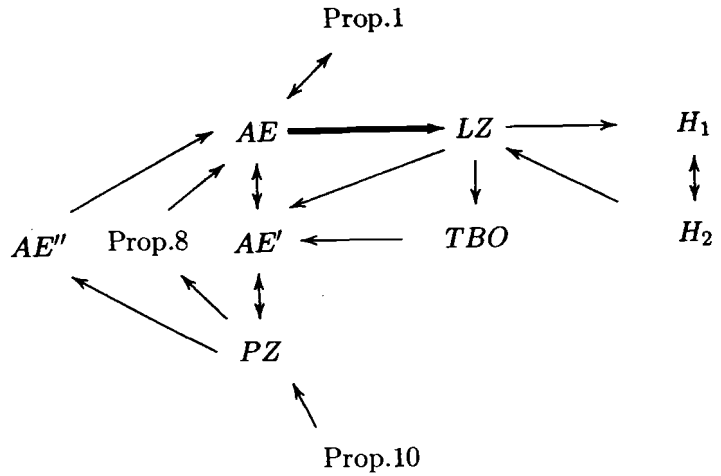
Hemos probado así que el lema de Zorn implica el teorema de la buena ordenación; demostremos que éste a su vez implica al axioma de elección AE' :

Sea X un conjunto no vacío; existe una relación $\leq$ de buen orden para X; si A es cualquier subconjunto no vacío de X, la función

$$e(A) = \text{primer elemento de } A$$

es de elección para X. □

Como resumen, elaboremos un diagrama de las equivalencias e implicaciones hasta ahora demostradas.



(Las proposiciones 8 y 10 son del capítulo anterior).

Ejercicios

1. Pruebe que si τ es una colección de conjuntos ordenada por inclusión y tal que la unión de toda cadena en τ también está en τ, entonces τ posee al menos un elemento maximal.

2. Demuestre que todo conjunto ordenado en el cual toda cadena tiene mínima cota superior, posee al menos un elemento maximal. Pruebe que a su vez esta propiedad implica alguno de los principios maximales vistos.

3. Si R es una relación de orden en X, demuestre que existe una relación de orden total S en X tal $R \subseteq S$. Ayuda: Aplique alguno de los principios maximales a la colección (ordenada por inclusión) de todas las relaciones de orden sobre X que contienen a R.

4. Pruebe que un conjunto X totalmente ordenado por R está bien ordenado por R si y sólo si para todo a de X, el conjunto $\sigma(a)$ de sus predecesores rigurosos está bien ordenado (por el orden inducido).

¿Es aplicable una condición tal a conjuntos parcialmente ordenados?

5. Un subconjunto A de un conjunto ordenado X se llama *cofinal en* X, si $(\forall x \in X)(\exists a \in A)(x \leq a)$.

   Demuestre que todo conjunto totalmente ordenado posee un subconjunto cofinal bien ordenado. Ayuda: Considere la colección de todos los subconjuntos de X bien ordenados por el orden inducido; ordene dicha colección por continuación; aplique el lema de Zorn y muestre que el subconjunto maximal hallado es cofinal en X.

6. Dé un ejemplo de un conjunto parcialmente ordenado que no posea un subconjunto cofinal bien ordenado.

7.2 ELECCIÓN Y CARDINALIDAD

Nos proponemos a continuación establecer algunos resultados más (generalizaciones de los casos particulares ya obtenidos) de aritmética cardinal.

TEOREMA 2 (Comparabilidad de cardinales.). *Si α y β son cardinales cualesquiera, entonces*

$$(\alpha \leq \beta) \vee (\beta \leq \alpha).$$

Como un corolario, después de las definiciones 6 y 7 y de la proposición 3 del capítulo VI, se obtiene la propiedad siguiente:

Tricotomía del orden entre Cardinales.

Para α, β cardinales cualesquiera, siempre se cumple una única de las relaciones

$$\alpha < \beta, \qquad \alpha = \beta, \qquad \beta < \alpha.$$

Demostración. (del teorema 2) Como todo número cardinal es el cardinal de un conjunto, existen conjuntos X, Y tales que $\alpha = \#(X)$, y $\beta = \#(Y)$. Es entonces suficiente probar que $(X \preceq Y) \vee (Y \preceq X)$, lo cual es equivalente a demostrar que existe una función inyectiva de uno de los dos conjuntos en el otro. En efecto:

La forma más sencilla de comparar el tamaño de los conjuntos X, Y es ir formando parejas ordenadas tomando el primer elemento en X y el segundo en Y, hasta que o bien se agoten simultáneamente los elementos de los dos conjuntos ($X \approx Y$), o bien se agoten los de X y no los de Y ($X \preceq Y$) o bien se agoten los de Y y no los de X ($Y \preceq X$). En los dos primeros casos el conjunto de parejas así formado es una inyección de X en Y y en el tercer caso el inverso de tal conjunto es una inyección de Y en X. Como para conjuntos infinitos nos es físicamente imposible formar parejas hasta agotar alguno de los dos conjuntos, necesariamente debemos utilizar el axioma de elección o alguna de sus formas equivalentes. Hagamos riguroso el raciocinio anterior: Supongamos $X \neq \emptyset \neq Y$, ya que si alguno de ellos es vacío, el resultado es trivial. Sean $a \in X$ y $b \in Y$; $F = \{(a, b)\}$ es una función inyectiva de un subconjunto de X sobre otro de Y. Sea F el conjunto de todas las extensiones inyectivas de f, es decir, la colección de todas las inyecciones g tales que $g \supseteq f$, $\mathcal{D}(g) \subseteq X$ y $\mathcal{R}(g) \subseteq Y$.

Ordenemos F por inclusión; si $\mathfrak{C}$ es una cadena en F es fácil ver que su unión $\bigcup_{g\in\mathfrak{C}} g$ también pertenece a F, de modo que por el lema de Zorn existe una extensión inyectiva h maximal.

Si existiesen $c \in X - \mathcal{D}(h)$ y $d \in Y - \mathcal{R}(h)$, es claro que la función $h^* = h \cup \{(c,d)\}$ sería una extensión estricta de h y ésta no sería maximal, luego $(\mathcal{D}(h) = X) \vee (\mathcal{R}(h) = Y)$. En el primer caso h es una inyección de X en Y y en el segundo h^{-1} es una inyección de Y en X, quedando demostrado el teorema. □

TEOREMA 3. Idempotencia de la adición de cardinales infinitos. *Si α es cualquier cardinal infinito, $\alpha + \alpha = \alpha$.*

Demostración. Sea A un conjunto cualquiera tal que $\alpha = \#(A)$; como $\#((A \times \{0\}) \cup (A \times \{1\})) = \alpha + \alpha$, es suficiente probar que $A \times \{0,1\} \approx A$.

Siendo A infinito, tendrá al menos un subconjunto D enumerable y por la proposición 11 del capítulo IV, $D \approx D \times \{0,1\}$, de manera que existirá al menos una biyección $u : D \to D \times \{0,1\}$.

Sea $\mathfrak{F}$ la colección de todas las funciones inyectivas f que extienden a u y tales que $\mathcal{D}(f) \subseteq A$ y $\mathcal{R}(f) = \mathcal{D}(f) \times \{0,1\}$. Como u está en $\mathfrak{F}$, entonces $\mathfrak{F} \neq \emptyset$ y claramente todas las funciones de $\mathfrak{F}$ tienen dominio infinito. Ordenemos $\mathfrak{F}$ por inclusión.

Sea $\mathfrak{C}$ una cadena en $\mathfrak{F}$; es simple rutina probar que $\cup\mathfrak{C}$ es una función inyectiva (ver ejercicio 13, sección 3, Cap.III); como

$$\begin{aligned}\mathcal{R}(\bigcup_{f\in\mathfrak{C}} f) = \bigcup_{f\in\mathfrak{C}} \mathcal{R}(f) &= \bigcup_{f\in\mathfrak{C}} (\mathcal{D}(f) \times \{0,1\}).\\ &= (\bigcup_{f\in\mathfrak{C}} \mathcal{D}(f)) \times \{0,1\}.\\ &= \mathcal{D}(\bigcup_{f\in\mathfrak{C}} f) \times \{0,1\}.\end{aligned}$$

también $\bigcup_{f\in\mathfrak{C}} f = \cup\mathfrak{C}$ está en $\mathfrak{F}$. El lema de Zorn implica entonces la existencia de una inyección h maximal en $\mathfrak{F}$; si $X = \mathcal{D}(h)$, afirmamos que $A - X$ es finito, ya que si fuese infinito, tendría un subconjunto Y numerable y existiría una biyección $g : Y \to Y \times \{0,1\}$; como $Y \cap X = \emptyset$, también son disyuntos los recorridos de h y g, luego por el teorema 8, sección 3 Cap. III, $h \cup g$ sería una función inyectiva y estando claramente en $\mathfrak{F}$, contradiría la maximalidad de h. Como $A = X \cup (A - X)$ y siendo X infinito y $A - X$ finito, entonces
$X \cup (A - X) \approx X$, luego $A \approx X$ y en consecuencia

$$A \times \{0,1\} \approx X \times \{0,1\} \approx X \approx A.$$

□

COROLARIO 1. *Si α y β son cardinales tales que al menos uno de ellos es infinito, entonces $\alpha + \beta = max\{\alpha, \beta\}$.*

Demostración. Sea γ el máximo entre α y β; evidentemente $\gamma \leq \alpha + \beta$ y como $(\alpha \leq \gamma) \wedge (\beta \leq \gamma)$, se tiene que $\alpha + \beta \leq \gamma + \gamma = \gamma$, luego por antisimetría del orden, $\alpha + \beta = \gamma$. □

TEOREMA 4. ***Idempotencia de la multiplicación de cardinales infinitos.***

Si α es cualquier cardinal infinito, $\alpha \cdot \alpha = \alpha$.

Demostración. Sea A tal que $\#(A) = \alpha$; sea $\mathfrak{B}$ la colección de todos los subconjuntos B de A tales que $B \times B \approx B$; $\mathfrak{B} \neq \emptyset$ ya que siendo A infinito posee subconjuntos B numerables los cuales satisfacen la propiedad requerida (proposición 11 Cap.VI); ordenemos $\mathfrak{B}$ por inclusión y dejemos al lector verificar que $\mathfrak{B}$ satisface las hipótesis del lema de Zorn (ver ejercicio 1), de modo que $\mathfrak{B}$ posee al menos un maximal X. La demostración queda completa si se prueba que $\#(A) = \#(X)$.

Supongamos que $\#(X) < \#(A)$; como $A = (A - X) \cup X$, $\#(A) = \#(A - X) + \#(X)$ y según el corolario anterior esta suma es el máximo de los dos y no pudiendo ser $\#(X)$ por la hipótesis, entonces $\#(A) = \#(A - X)$, lo cual significa que X es equipotente a algún subconjunto Y de $A - X$, y puesto que $X \times X \approx X$, también $Y \times Y \approx Y$. Siendo Y y X disyuntos, los conjuntos $X \times X$, $X \times Y$, $Y \times X$ y $Y \times Y$ son disyuntos dos a dos y entonces

$$\begin{aligned}\#[(X \cup Y) \times (X \cup Y)] &= \#[(X \times X) \cup (X \times Y) \cup (Y \times X) \cup (Y \times Y)]\\ &= \#(X \times X) + \#(X \times Y) + \#(Y \times X) + \#(Y \times Y)\\ &= \#(X \times X) + \#(X \times X) + \#(X \times X) + \#(Y \times Y)\\ &= \#(X) + \#(X) + \#(X) + \#(Y)\\ &= \#(X) + \#(Y)\\ &= \#(X \cup Y).\end{aligned}$$

Concluimos que $(X \cup Y) \times (X \cup Y) \approx (X \cup Y)$ y X no sería maximal.

El lector debe justificar las igualdades anteriores. □

COROLARIO 2. *Si uno al menos de los cardinales α y β es infinito y el otro no es cero, entonces $\alpha \cdot \beta = max\{\alpha, \beta\}$.*

COROLARIO 3. *Si uno al menos de los cardinales α y β es infinito y el otro no es cero, entonces $\alpha + \beta = \alpha\beta$.*

Dejamos sus demostraciones como ejercicio.

Ejercicios

1. Sea $\mathfrak{B}$ una colección de conjuntos B tales que $B \times B \approx B$; ordenemos $\mathfrak{B}$ por inclusión y tomemos una cadena $\mathfrak{C}$ en $\mathfrak{B}$. Demuestre que $\cup\mathfrak{C}$ también está en $\mathfrak{B}$.

   Ayuda: Si $B \times B \approx B$, entonces $\bigcup_{B\in\mathfrak{C}} B \approx \bigcup_{B\in\mathfrak{C}}(B \times B)$ y éste claramente es un subconjunto de $(\bigcup_{B\in\mathfrak{C}} B) \times (\bigcup_{B\in\mathfrak{C}} B)$, así que basta demostrar que este producto está contenido en $\bigcup_{B\in\mathfrak{C}}(B \times B)$.

2. Pruebe los dos últimos corolarios del teorema 3 anterior.

3. Si α es un cardinal infinito y $n \in \mathbb{N}$,

   (a) pruebe que $\alpha^n = \alpha$. Concluya que si A es un conjunto infinito, $A^n \approx A$.

   (b) Pruebe que la colección de todas las sucesiones finitas de elementos de A, también es equipotente con A.

   (c) Si $\mathcal{P}_n(A) = \{B \mid B \subseteq A \wedge \#(B) = n\}$, demuestre que $\mathcal{P}_n(A) \preceq A^n$. Concluya que $\#(\mathcal{P}_n(A)) = \#(A)$.

   (d) Pruebe que la colección $\mathcal{P}_F(A)$ de todos los subconjuntos finitos de A tiene el mismo cardinal que A.

4. Si $\alpha = 2^\beta$, entonces $(\forall\gamma \leq \beta)(\alpha^\gamma = \alpha)$.

5. Si $\#(A) = 2^\beta$, pruebe que $\{B \mid B \subseteq A \wedge \#(B) \leq \beta\} \approx A$.

6. Como una inquietud, averigüe cinco resultados de álgebra, análisis o topología en cuyas demostraciones se utilice el axioma de elección o alguno de los principios maximales equivalentes.

7. Si X es un conjunto infinito, pruebe que para todo subconjunto A de X se cumple que

$$A \approx X \quad \text{ó} \quad (X - A) \approx X.$$

8. Demuestre que todo conjunto infinito X puede obtenerse como unión disyunta de dos subconjuntos equipotentes con X.

   Ayuda: $(X \times \{0\}) \cup (X \times \{1\}) \approx X \times X \approx X$; use una biyección de esta unión disyunta sobre X.

7.3 EL AXIOMA DE FUNDAMENTACIÓN

Aun cuando no es un axioma que tenga un papel esencial en el cuerpo de la matemática, en el sentido de que su supresión pueda ocasionar la pérdida de porciones importantes de ella, sí es de gran interés. en el estudio de la fundamentación de la misma teoría de conjuntos. Dicho axioma implica propiedades muy deseables de la estructura interna de los conjuntos, para que éstos concuerden en lo posible con las ideas intuitivas que de ellos poseemos. Por ejemplo, la experiencia que hemos adquirido en el manejo de los conjuntos nos lleva a concluir que no existe un conjunto que sea elemento de sí mismo; en la capítulo III logramos probar que $(\forall n \in \mathbb{N})(n \notin n)$; sin embargo, no podemos demostrar que esta propiedad la posean todos los conjuntos, o a no ser que dispongamos del axioma de fundamentación. Tampoco hemos hallado dos conjuntos tales que cada uno de ellos sea elemento del otro.

Nuestra intuición divide el universo conjuntista en estratos: el más bajo está constituido por los individuos y son los elementos más simples, pudiendo no existir, como en el caso de la teoría que hemos desarrollado. El segundo estrato lo constituyen los conjuntos de individuos (tan solo $\emptyset$ en nuestro caso) y son los conjuntos más simples. El tercer estrato está constituido por conjuntos cuyos elementos pertenecen a los dos estratos anteriores, y así sucesivamente.

Para que pueda probarse esta estratificación de los conjuntos, se requiere del axioma de fundamentación.

Cuando los elementos de un conjunto poseen dicha estratificación, se dice que *el conjunto es bien fundamentado.* De ahí proviene el nombre del axioma y su propósito es afirmar que *todo conjunto es bien fundamentado.*

Este axioma aparece por primera vez en 1917 en un trabajo de D. Mirimanoff; en 1925 J. Von Newmann le da estatus al incluirlo dentro de los axiomas de su teoría de conjuntos y en 1930, E. Zermelo da la versión usada hoy en día:

(AF) : *Si X es un conjunto no vacío, entonces X posee un elemento μ tal que $\mu \cap X = \emptyset$.*

En el lenguaje objeto de la teoría de conjuntos sería:

$$(\forall X)(X \neq \emptyset \rightarrow (\exists \mu)(\mu \in X \wedge \mu \cap X = \emptyset)).$$

Inmediatamente obtenemos dos de las consecuencias anunciadas:

PROPOSICIÓN 1. $(\forall X)(X \notin X)$.

Si existe un conjunto A tal que $A \in A$, formemos el conjunto $X = \{A\}$. Es no vacío y contradice el axioma de fundamentación ya que $A \cap X \neq \emptyset$ puesto que $A \in X$ y $A \in A$.

PROPOSICIÓN 2. *No existen dos conjuntos A, B tales que $A \in B$ y $B \in A$.*

Si existiesen, consideraríamos el conjunto $X = \{A, B\}$. Es claro que $A \cap X \neq \emptyset$ ya que $B \in A \wedge B \in X$. Análogamente, $B \cap X \neq \emptyset$ ya que $A \in B \wedge A \in X$. El conjunto X contradiría el axioma de fundamentación.

Generalizando:

PROPOSICIÓN 3. *No existen conjuntos $A_1, A_2, \cdots, A_n$ tales que* $(A_1 \in A_2) \wedge (A_2 \in A_3) \wedge \cdots \wedge (A_{n-1} \in A_n) \wedge (A_n \in A_1)$.

Si existiesen, el conjunto $X = \{A_1, A_2, \cdots, A_n\}$ contradiría el axioma de fundamentación ya que

$$A_n \in (A_1 \cap X) \quad \text{y} \quad (\forall i = 2, 3, \cdots, n)(A_{i-1} \in (A_i \cap X)).$$

La definición de cardinal dada por Frege (ver Cap. IV, sección 1) entraría en contradicción con el axioma de fundamentación, ya que si existiese el conjunto "3" constituido por todos los conjuntos con tres elementos, es decir, $3 = \{A \mid A \approx \{a, b, c\}\}$, entonces el conjunto $X = \{3, b, c\}$ sería tal que 3 estaría en X y también X estaría en 3 ya que $X \approx \{a, b, c\}$, contradiciendo la proposición 2. Así sale a flote un problema más que lleva consigo dicha definición de cardinal.

Volviendo a la estratificación intuitiva que poseen los elementos de un conjunto, si la miramos de arriba hacia bajo, la buena fundamentación de un conjunto significa que sus elementos son de estratos más bajos que los del conjunto, y a su vez los elementos de sus elementos son de estratos más bajos que los de los elementos del conjunto $\cdots$ hasta llegarse en finitos pasos al conjunto más simple ($\emptyset$) o a los elementos más simples (los individuos). Esto significa que

PROPOSICIÓN 4. *No es posible hallar una sucesión infinita de conjuntos $S_0, S_1, \cdots$ tales que*

$$(\forall k \in \mathbb{N})(S_{k+1} \in S_k),$$

es decir, no existe una sucesión

$$S_0 \ni S_1 \ni S_2 \ni S_3 \ni \cdots \ni S_n \ni S_{n+1} \ni \cdots$$

A una sucesión de este tipo se le llama una *cadena descendente infinita.*

Demostración. Si existiese una sucesión tal, sea X el conjunto de los elementos de dicha sucesión:

$$X = \{S_k \mid k \in \mathbb{N}\}$$

para cualquier k en $\mathbb{N}$ se tiene que $S_{k+1} \in (S_k \cap X)$ y se entraría en contradicción con el axioma de fundamentación ya que ningún elemento de X tendría intersección vacía con X. □

Es igualmente sencillo probar que en presencia del axioma de elección, la proposición 4 implica a su vez al axioma de fundamentación (AF). En lugar de demostrar "Prop. 4 $\Rightarrow$ AF" se prueba (es más fácil) "$\neg$AF $\Rightarrow \neg$Prop. 4". En efecto, si $(\exists X)(X \neq \emptyset \wedge (\forall \mu)(\mu \in X \rightarrow \mu \cap X \neq \emptyset))$, sean $X_0 = X$ y $X_1 \in X_0$.

Como $X_1 \cap X_0 \neq \emptyset$, sea $X_2 \in X_1 \cap X_0$. Puesto que $X_2 \in X_0$, entonces $X_2 \cap X_0 \neq \emptyset$; sea $X_3 \in (X_2 \cap X_0)$. Como $X_3 \in X_0$, entonces $X_3 \cap X_0 \neq \emptyset$; sea $X_4 \in (X_3 \cap X_0)$.

$$\vdots$$

Repitiendo este proceso tantas veces como números naturales, (aquí estamos usando el axioma de elección), se obtiene una cadena descendente infinita

$$X_0 \ni X_1 \ni X_2 \ni X_3 \ni \cdots$$

quedando probado "$\neg$Prop. 4".

Si observamos de abajo hacia arriba la estratificación de los conjuntos, el más simple es el vacío; él solo constituye un estrato; notémoslo V_1 (ya que V_0 sería el conjunto de los individuos y en nuestra teoría no los hay). Así

$$V_0 = \emptyset \quad \text{y} \quad V_1 = \{\emptyset\}.$$

El siguiente estrato V_2 estaría constituido por conjuntos cuyos elementos pertenecen a los estratos anteriores:

$$V_2 = \{\emptyset, \{\emptyset\}\}, \quad \text{resultando ser} \quad \mathcal{P}(V_1).$$

El estrato siguiente V_3 sería $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$ o sea $\mathcal{P}(V_2)$. Observemos que $V_0 \subset V_1 \subset V_2 \subset V_3$, y en general, $V_i \subset V_{i+1}$, de manera que para formar V_{n+1} bastará construir conjuntos cuyos elementos pertenezcan a V_n, es decir, bastará construir subconjuntos de V_n, luego $V_{n+1} = \mathcal{P}(V_n)$.

Si notamos por V_k a la colección de conjuntos del estrato k, es claro que puede definirse inductivamente:

$$V_0 = \emptyset$$
$$V_{n+1} = \mathcal{P}(V_n), \quad \text{para todo } n \in \mathbb{N}$$

Como $\#(V_{n+1}) = \#(\mathcal{P}(V_n)) = 2^{\#(V_n)}$ y V_0 es finito, entonces todos los V_n serán finitos.

El estrato que está "inmediatamente después " de todos los V_n estará constituido por todos los conjuntos que pueden formarse tomando elementos de los distintos V_n. Después de pensarlo un poco, se llega a la conclusión que debe coincidir con la unión de todos los V_n ; es costumbre notarlo V_ω. Así

$$V_\omega = \bigcup_{n \in \mathbb{N}} V_n.$$

El siguiente estrato será $V_{\omega+1}$ y se continúa con $V_{\omega+2}$, $V_{\omega+3}$, ... Aquí también $V_{\omega+n+1} = \mathcal{P}(V_{\omega+n})$ y además

$$V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_\omega \subset V_{\omega+1} \subset V_{\omega+2} \subset \cdots$$

De manera análoga, después de todos los $V_{\omega+n}$ está $\bigcup_{n \in \mathbb{N}} V_{\omega+n}$, que se acostumbra notar $V_{\omega 2}$. Podemos entonces alargar nuevamente la sucesión de estratos

$$V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_\omega \subset V_{\omega+1} \subset V_{\omega+2} \subset \cdots \subset V_{\omega 2} \subset V_{\omega 2+1} \subset V_{\omega 2+2} \cdots$$

Nótese que si por ejemplo $A \in V_5$, entonces A también estará en todos los estratos posteriores, de manera que lo que realmente mide la complejidad de un conjunto es el estrato en el cual el conjunto *aparece por primera vez*; si $A \in V_\alpha$ y $A \notin V_{\alpha-1}$, se puede decir que A es de complejidad α. Es costumbre llamar a α *el rango de* A y notarlo $\alpha = \rho(A)$. Por ejemplo, el número $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$ aparece por primera vez como elemento en V_3, luego el rango de "2" es 3.

Las consideraciones anteriores, además de mostrarnos un poco la estructura de los conjuntos cuando vale el axioma de fundamentación, ponen de presente la necesidad de saber algunas cosas sobre los números ordinales para poder continuar analizando la estratificación, ya que debemos usarlos como subíndices para etiquetar los estratos.

Ejercicios

1. Sea $(X, \leq)$ un conjunto ordenado; una *cadena descendente infinita* de X es una sucesión infinita donde cada término precede estrictamente al anterior: $\cdots x_3 < x_2 < x_1 < x_0$.

   Demuestre que un conjunto totalmente ordenado que no posee cadenas descendentes infinitas es bien ordenado.

2. Compruebe que $3 = \{0, 1, 2\}$ está en V_4 y no en V_3, de modo que $\rho(3) = 4$.

3. Demuestre por inducción que $(\forall n \in \mathbb{N})(\rho(n) = n + 1)$.

4. Si $A = \{x_1, x_2, x_3, \cdots, x_n\}$ es un subconjunto finito de $\mathbb{N}$ y l es el máximo (para el orden usual) elemento de A, pruebe que todos los elementos de A aparecen simultáneamente por primera vez, cuando aparece el máximo, es decir, en V_{l+1}, de modo que $\rho(A) = l + 2$.

5. Recordemos que (a, b)=$\{\{a\}, \{a, b\}\}$. ¿Cuál será el rango de $(2, 4)$? ¿y el de (4,2)? ¿y el de (3,3)?

6. Si $m \neq n$ y l =máx$\{m, n\}$, pruebe que tanto (m, n) como (n, m) tienen rango $l + 3$. ¿Cuál será el rango de (n, n)?

7. (a) Demuestre que todo conjunto que esté en V_w, es finito.
   (b) Pruebe que ningún conjunto tiene rango w, ya que si aparece en V_w, necesariamente ha aparecido antes en algún V_n.
   (c) Análogamente, muestre que ningún conjunto tiene rango $w2$.

8. ¿Cuál será el rango del conjunto $\mathbb{N}$ de los naturales? ¿y cuál será el rango de $\mathbb{N} \times \mathbb{N}$?

9. Dé un conjunto unitario de rango 3 y otro unitario de rango $w + 2$, para hacer ver que $A \approx B$ no implica $\rho(A) = \rho(B)$.

10. Pruebe que si $\rho(A) = \alpha < w2$, entonces existe β tal que $\alpha = \beta + 1$.

11. Demuestre que si $\rho(A) = \alpha < w2$, entonces todos los elementos de A tienen rango menor que α. Ayuda: Use el ejercicio anterior y recuerde que $V_{\beta+1} = \mathcal{P}(V_\beta)$.

12. Si $\rho(A) = \alpha$ y $B \subseteq A$, pruebe que $\rho(B) \leq \alpha$.

13. Si f es una función de $\mathbb{N}$ en $\mathbb{N}$, halle su rango $\rho(f)$.

    Ayuda: $f \subset \mathbb{N} \times \mathbb{N}$.

*14. (a) En el capítulo V se construyó $\mathbb{Z}$ como $\mathbb{N} \times \mathbb{N} / \approx$; halle $\rho(\mathbb{Z})$.
    (b) También se construyó $\mathbb{Q}$ como $\mathbb{Z} \times \mathbb{Z}^* / \simeq$; halle $\rho(\mathbb{Q})$.
    (c) En el mismo capítulo se construyó $\mathbb{R}$ como conjunto de cortaduras, es decir, como conjunto de colas a izquierda de racionales. ¿Cuál es el rango de $\mathbb{R}$ así construido?

    Si es de su interés, averigüe cuál es el rango de $\mathbb{R}$ cuando se construye como conjunto de clases de equivalencia de sucesiones de Cauchy de racionales, y compárelo con el rango de $\mathbb{R}$ obtenido antes.

7.4 EL AXIOMA DE REEMPLAZO

En 1922, de manera independiente y casi simultánea, **Toralf Skolem** y **Abraham Fraenkel**, modificaron el sistema axiomático propuesto por Zermelo para la teoría de conjuntos, cambiando el axioma de separación por el de reemplazo o sustitución, con el fin de hacer la teoría adecuada para el tratamiento de la aritmética ordinal y de la definición por recurrencia transfinita.

El axioma de separación tiene como finalidad limitar el tamaño de los conjuntos que pueden formarse lícitamente; el axioma de reemplazo persigue el mismo fin pero es de naturaleza un poco diferente: *si $\varphi(x,y)$ es una relación funcional en x* (o como se llamó antes, una condición en dos variables, o sea una fórmula bien formada del lenguaje objeto de la teoría de conjuntos, tal que para a,b,c cualesquiera, $\varphi(a,b) \wedge \varphi(a,c) \rightarrow b = c$) y *$A$ es un conjunto*, el axioma afirma que *existe un conjunto B cuyos elementos son precisamente las imágenes bajo esta relación funcional de aquellos elementos de A que estén en el dominio de φ*. En el lenguaje de la teoría de conjuntos sería:

Axioma de reemplazo: *Para cada $\varphi(x,y,z_1,\cdots,z_n)$ fórmula bien formada con $x,y,z_1,\cdots,z_n$ como únicas variables libres (distintas todas ellas), la siguiente fórmula es un axioma:*

$$\forall z_1 \cdots \forall z_n \{\forall x \forall y \forall y' [\varphi(x,y,z_1,\cdots,z_n) \wedge \varphi(x,y',z_1,\cdots,z_n) \rightarrow y = y'] \rightarrow \forall A \exists B \forall v [v \in B \leftrightarrow \exists u (u \in A \wedge \varphi(u,v,z_1,\cdots,z_n))]\}.$$

Nótese que este es un esquema, un molde para producir axiomas, uno por cada φ.

Este axioma implica al de separación: Dada una fórmula $\psi(x,z_1,\cdots,z_n)$, si tomamos como $\varphi(x,y,z_1,\cdots,z_n)$ a la relación $y = x \wedge \psi(x,z_1,\cdots,z_n)$, observamos que ésta es funcional en x, luego

$$\forall z_1 \cdots \forall z_n \{\forall A \; \exists B \; \forall v [v \in B \leftrightarrow (\exists u)(u \in A \wedge v = u \wedge \psi(u,z_1,\cdots,z_n))]\}$$

Pero

$$(\exists u)(u \in A \wedge v = u \wedge \psi(u,z_1,\cdots,z_n))$$

es en realidad $v \in A \wedge \psi(v,z_1,\cdots,z_n))$, luego

$$\forall z_1 \cdots \forall z_n [\forall A \; \exists B \; \forall v [v \in B \leftrightarrow v \in A \wedge \psi(v,z_1,\cdots,z_n))]$$

que es el axioma de separación de Zermelo.

Es fundamental que la relación φ del axioma de reemplazo sea funcional; por ejemplo, la relación $\varphi(x,y) : x \subseteq y$ no es funcional en x ya que un x puede ser subconjunto de muchos y. Si aplicáramos el axioma tomando como $A = \{\emptyset\}$, se tendría

$$(\exists B)(\forall v)(v \in B \leftrightarrow (\exists u)(u \in \{\emptyset\} \wedge u \subseteq v))$$

$$\text{o sea} \quad (\exists B)(\forall v)(v \in B \leftrightarrow \emptyset \subseteq v)$$

y B sería el inexistente conjunto de todos los conjuntos, ya que todo conjunto contiene al vacío como subconjunto.

Al agregarse el axioma de sustitución, también puede suprimirse el axioma del conjunto con dos elementos, ya que es derivable como teorema; en efecto, si c,b son dados y queremos formar $\{c,b\}$, aplicando a $\emptyset$ el axioma del conjunto de partes dos veces, obtenemos $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset,\{\emptyset\}\}$, el cual es un conjunto con dos elementos. para aplicar el axioma de reemplazo, elijamos como A al conjunto binario $\{\emptyset,\{\emptyset\}\}$ y como $\varphi(x,y)$ a la fórmula $(x = \emptyset \wedge y = c) \vee (x = \{\emptyset\} \wedge y = b)$. Es funcional en x por que para cada valor de x en $\mathcal{P}(\mathcal{P}(\emptyset))$, hay exactamente una y que verifica φ, y para otros valores de x, no existen valores de y que verifiquen φ. El axioma de sustitución viene a ser en este caso

$(\exists B)(\forall v)(v \in B \leftrightarrow (\exists u)(u \in \{\emptyset,\{\emptyset\}\} \wedge [(u = \emptyset \wedge v = c) \vee (u = \{\emptyset\} \wedge v = b)]))$

de donde se deduce

$(\exists B)(\forall v)(v \in B \leftrightarrow (v = c \vee v = b))$ es decir, $B = \{c,b\}$.

Otro problema aún no resuelto, es el siguiente: En el capítulo IV, sección 3, ejercicio 10, se preguntaba si usando algún principio de definición por recurrencia, era posible determinar una función μ de dominio $\mathbb{N}$ tal que:

1. $\mu(0) = A$ y
2. $(\forall n)(\mu(n+1) = \mathcal{P}(\mu(n)))$.

Es claro que aplicando el axioma del conjunto de partes, podemos a partir de A, formar $\mathcal{P}(A), \mathcal{P}(\mathcal{P}(A)), \mathcal{P}(\mathcal{P}(\mathcal{P}(A))) \cdots$

En general para n un número natural, podemos formar $\mathcal{P}^n(A)$, o sea el conjunto obtenido a partir de A tomando partes iteradamente n veces.

El problema de la definición de la función μ radica en que no poseemos un conjunto que contenga a todos los $\mathcal{P}^n(A)$ para todo n natural, y en consecuencia no podemos definir una función "partes", $\mathcal{P} : B \rightarrow B$, para algún conjunto B adecuado, que sirva a la vez como conjunto de llegada de la función $\mu : \mathbb{N} \rightarrow B$. El axioma de reemplazo nos permite solucionar

este problema: si tomamos como $\varphi(x,y)$ a "$x \in \mathbb{N} \wedge y = \mathcal{P}^x(A)$", es claramente una relación funcional en x de manera que para $A = \mathbb{N}$ se obtiene $(\exists B)(\forall v)(v \in B \leftrightarrow (\exists u)(u \in \mathbb{N} \wedge u \in \mathbb{N} \wedge v = \mathcal{P}^u(A)))$

y simplificando $(\exists B)(\forall v)(v \in B \leftrightarrow (\exists u)(u \in \mathbb{N} \wedge v = \mathcal{P}^u(A)))$.

Luego B es el conjunto que estábamos buscando, ya que es precisamente $B = \{A\ (= \mathcal{P}^0(A)), \mathcal{P}(A), \mathcal{P}(\mathcal{P}(A)), \cdots, \mathcal{P}^n(A), \cdots\}$.

En el próximo capítulo se hará uso del axioma de reemplazo para manejar adecuadamente los números ordinales.

Ejercicios

1. Use el axioma de reemplazo para demostrar la existencia del conjunto $C = \{A, A \times A, (A \times A) \times A, \cdots, A^n, \cdots\}$.

2. Pruebe que existe el conjunto $\{A, \{A\}, \{\{A\}\}, \{\{\{A\}\}\}, \cdots\}$.

**

Capítulo 8

NUMEROS ORDINALES

Para atar algunos cabos sueltos y despertar el interés del lector por el estudio de ciertos temas complementarios, presentaremos en este capítulo las propiedades fundamentales de los números ordinales y sus relaciones con los axiomas de reemplazo y elección.

8.1 ÓRDENES SEMEJANTES

¿Cuándo dos conjuntos ordenados son esencialmente el mismo?

En esta sección queremos responder parcialmente la pregunta anterior y obtener de dicha respuesta algunas consecuencias de utilidad posterior.

Recordemos que un conjunto ordenado es una pareja (A, R) en la cual A es un conjunto y R (subconjunto de $A \times A$) es un orden para A. Así un conjunto ordenado es una estructura muy sencilla: consta de un universo (el conjunto A) y una relación binaria R que es un orden para A.

Se sabe que dos estructuras del mismo tipo son *isomorfas*, cuando existe una biyección entre sus universos que *preserva* las operaciones y relaciones de dichas estructuras. En este orden de ideas, dos conjuntos ordenados son esencialmente el mismo cuando son isomorfos desde este punto de vista, es decir, cuando existe una biyección entre sus universos que preserva el orden. Se acostumbra decir en este caso que los dos conjuntos ordenados

son semejantes.

DEFINICIÓN 1. *Un conjunto ordenado (A, R) es semejante a otro conjunto ordenado (B, S) si existe una biyección $f : A \to B$ tal que*

$$(\forall x, y \in A)(xRy \leftrightarrow f(x)Sf(y)) \text{ o equivalentemente,}$$

$$(\forall x, y \in A)((x, y) \in R \leftrightarrow (f(x), f(y)) \in S).$$

En esta última expresión estamos haciendo énfasis en las relaciones como conjuntos de parejas, y ella es equivalente a $(f \times f)(R) = S$.

Escribiremos $(A, R) \cong (B, S)$ para indicar que (A, R) es semejante a (B, S) y a f la llamaremos una semejanza. Debido a que $f : A \to B$ es una biyección, también $f^{-1} : B \to A$ lo es y $(f^{-1} \times f^{-1})(S) = R$, luego f^{-1} también es una semejanza y en consecuencia "ser semejante a" es una relación simétrica.

Es sencillo demostrar que la composición de semejanzas es una semejanza y trivial que la identidad de un conjunto ordenado es una semejanza. Se concluye que "x es semejante a y" es una relación de equivalencia en cualquier colección de conjuntos ordenados. En particular, dado un conjunto no vacío E, si formamos la colección $\mathcal{O}(E)$ de todos los conjuntos ordenados (A, R) con $A \subseteq E$, la relación de semejanza particiona $\mathcal{O}(E)$ en clases de equivalencia constituidas por conjuntos ordenados semejantes.

Recordemos que si "$\preceq$" es un orden para A, su orden estricto asociado "$\prec$" está definido mediante

$$a \prec b \leftrightarrow a \preceq b \wedge a \neq b.$$

Si $f : (A, \preceq) \longrightarrow (B, \preceq)$ es una semejanza, ésta preserva el orden estricto, es decir, $(\forall x, y \in A)(x \prec y \leftrightarrow f(x) \prec f(y))$ (dejamos al lector la tarea de probarlo). La afirmación recíproca "si $f : A \to B$ es una biyección y preserva el orden estricto, entonces $f : (A, \preceq) \longrightarrow (B, \preceq)$ es una semejanza", también es cierta e igualmente dejamos su demostración al lector.

Sean $(A, \preceq)$ un conjunto ordenado y $a \in A$; el *segmento inicial* determinado por a, es el conjunto $\sigma(a) = \{x \in A \mid x \prec a\}$. Un resultado natural de utilidad posterior, es el siguiente:

PROPOSICIÓN 1. *Sean A, B conjuntos totalmente ordenados y sean $a, b \in A$; supongamos que $f : \sigma(a) \longrightarrow \sigma(b)$ es una semejanza; entonces para todo $x \in \sigma(a)$ se tiene que $\sigma(x) \cong \sigma(f(x))$, siendo esta última semejanza establecida por la restricción $f \restriction \sigma(x)$.*

Demostración. : Claramente $f \restriction \sigma(x) : \sigma(x) \longrightarrow \sigma(b)$ es inyectiva y preserva el orden. Además si $z \in \sigma(x)$, entonces $z \prec x$ y en consecuencia $f(z) \prec f(x)$, luego $f(z) \in \sigma(f(x))$, o sea que $f(\sigma(x)) \subseteq \sigma(f(x))$. La proposición queda demostrada si probamos que $\sigma(f(x)) \subseteq f(\sigma(x))$. En efecto, si $y \in \sigma(f(x))$, entonces $y \prec f(x) \prec b$ y como f es sobreyectiva, existe $z \in \sigma(a)$ tal que $f(z) = y$. Si fuese $z \succeq x$ se tendría $f(z) = y \succeq f(x)$ contrario a la relación ya establecida, luego $z \prec x$, o sea $z \in \sigma(x)$ y así $y = f(z) \in f(\sigma(x))$, quedando demostrado. □

DEFINICIÓN 2. *Sea $(A, \preceq)$ un conjunto ordenado; un subconjunto S de A se llama una* sección *de A si todo predecesor de un elemento de S también está en S.*

PROPOSICIÓN 2. *Las únicas secciones de un conjunto bien ordenado, son el conjunto completo y sus segmentos iniciales.*

Demostración. Es claro que el conjunto completo A y sus segmentos iniciales son secciones. Recíprocamente, sea S una sección, $S \neq A$ y mostremos que es un segmento inicial; $A - S \neq \emptyset$ luego posee primer elemento, digamos b; entonces $\sigma(b) \subseteq S$; si $S - \sigma(b) \neq \emptyset$, sea $x \in (S - \sigma(b))$; Claramente $(x \in S) \wedge (x \geq b)$ y como S es una sección, b estará en S, en contradicción con $b \in (A - S)$. Se concluye que $S = \sigma(b)$. □

Una función inyectiva de un conjunto ordenado en sí mismo que preserve el orden, es en particular *estrictamente creciente*: $x \prec y \to f(x) \prec f(y)$; sin embargo no podemos afirmar que $x \preceq f(x)$, ni lo contrario. Por ejemplo si consideramos el conjunto $\mathbb{Z}$ de los enteros con su orden usual, las funciones $f, g : (\mathbb{Z}, \leq) \longrightarrow (\mathbb{Z}, \leq)$ definidas por $f(x) = x + 5$ y $g(x) = x - 6$ son autosemejanzas de $(\mathbb{Z}, \leq)$ y a pesar de ser este conjunto totalmente ordenado, $(\forall x)(x < f(x))$ y $(\forall x)(x > g(x))$.

La situación cambia radicalmente cuando el conjunto es bien ordenado:

PROPOSICIÓN 3. *Si $f : (A, \preceq) \longrightarrow (A, \preceq)$ es inyectiva y preserva el orden y si $(A, \preceq)$* es bien ordenado, *entonces $(\forall x \in A)(x \preceq f(x))$.*

Demostración. : Si existiesen elementos y tales que $f(y) \prec y$, el conjunto $B = \{y \in A | f(y) \prec y\}$ no sería vacío y por consiguiente tendría un primer elemento b. Así $f(b) \prec b$ pero por esto mismo $f(b)$ no estaría en B, luego $f(b) \preceq f(f(b))$. De otra parte como $f(b) \prec b$ y f conserva el orden estricto, $f(f(b)) \prec f(b)$, obteniéndose una contradicción. En consecuencia B deberá ser vacío , es decir, $(\forall x \in A)(x \preceq f(x))$. □

Este comportamiento especial de los conjuntos bien ordenados facilita muchísimo el análisis de la estructura de dichos conjuntos. Por esto en adelante nos dedicaremos a estudiar la semejanza tan solo entre conjuntos bien ordenados; por ejemplo, una consecuencia inmediata es la siguiente:

PROPOSICIÓN 4. *Si dos conjuntos bien ordenados son semejantes, entonces existe una única semejanza entre ellos.*

Demostración. : Sean $f, g : (A, \preceq) \longrightarrow (B, \preceq)$ semejanzas entre conjuntos bien ordenados; también f^{-1} y g^{-1} son semejanzas, de modo que tanto $g^{-1} \circ f$ como $f^{-1} \circ g$ son autosemejanzas de $(A, \preceq)$, luego por la proposición anterior, $(\forall x \in A)(x \preceq (g^{-1} \circ f)(x))$ y $(\forall x \in A)(x \preceq (f^{-1} \circ g)(x))$ y aplicando g a los dos lados en el primer caso y f a los dos lados en el segundo,$(\forall x \in A)(g(x) \preceq f(x))$ y $(\forall x \in A)(f(x) \preceq g(x))$, de modo que $(\forall x \in A)(f(x) = g(x))$, es decir $f = g$. □

COROLARIO 1. *La única autosemejanza de un conjunto bien ordenado es la identidad.*

Esto no impide que existan semejanzas entre un conjunto bien ordenado y algunos de sus subconjuntos propios; por ejemplo $f(n) = 2n$ es una semejanza entre $\mathbb{N}$ y su subconjunto de los naturales pares. Sin embargo,

PROPOSICIÓN 5. *Un conjunto bien ordenado nunca es semejante a un subconjunto de uno de sus segmentos iniciales.*

Demostración. Por contradicción: Sea $(A, \preceq)$ bien ordenado y supongamos que existen $a \in A$ y $B \subseteq \sigma(a)$ tales que $f : A \longrightarrow B$ es una semejanza; si extendemos el codominio B de f a A, entonces $f : A \longrightarrow A$ es una función inyectiva que preserva el orden, luego por la proposición 3 se tiene $a \preceq f(a)$ y esto hace que $f(a) \notin \sigma(a)$, contrario a la hipótesis de que el recorrido de f es un subconjunto de $\sigma(a)$. □

COROLARIO 2. *Un conjunto bien ordenado nunca es semejante a uno de sus segmentos iniciales.*

Basta tomar en la prueba anterior $B = \sigma(a)$.

PROPOSICIÓN 6. *Sean $(A, \preceq)$ y $(B, \preceq)$ conjuntos bien ordenados; si A es semejante a un segmento inicial de B. entonces B no puede ser semejante a un subconjunto de A.*

Demostración. Sea $f : A \longrightarrow \sigma(b)$ una semejanza entre A y un segmento inicial de B. Supongamos que existiera una semejanza $g : B \longrightarrow C$ con $C \subseteq A$; entonces $f \circ g : B \longrightarrow \sigma(b)$ sería inyectiva y preservaría el orden y en consecuencia $B \cong (f \circ g)(B) \subseteq \sigma(b)$, en contradicción con la proposición 5. □

TEOREMA 1. (de comparación de conjuntos bien ordenados) *Dados dos conjuntos bien ordenados cualesquiera, o son semejantes o uno de ellos es semejante a un segmento inicial del otro.*

Con más precisión: Dados $(A, \preceq)$ y $(B, \preceq)$ bien ordenados, siempre se cumple uno de lo tres casos siguientes:

(i) $(A, \preceq) \cong (B, \preceq)$.

(ii) $(\exists b \in B)((A, \preceq) \cong \sigma(b))$.

(iii) $(\exists a \in A)((\sigma(a) \cong (B, \preceq))$.

Demostración. : Supongamos A y B no vacíos; definamos al conjunto $A_0 = \{x \in A | (\exists y \in B)(\sigma(x) \cong \sigma(y)\}$. Este conjunto no es vacío ya que si a es el primer elemento de A y b es el primero de B, entonces $\sigma(a) \cong \sigma(b)$ (son vacíos). Sea $x \in A_0$ y sea y en B tal que $\sigma(a) \cong \sigma(y)$. Si existiese otro z en B con $z \neq y$ y tal que $\sigma(a) \cong \sigma(z)$, entonces por transitividad y simetría, $\sigma(y) \cong \sigma(z)$; pero $y \prec z$ o $z \prec y$; en el primer caso $\sigma(z)$ será semejante a uno de sus segmentos iniciales, en contradicción con el corolario de la proposición 5; lo mismo sucede si $z \prec y$.

Se concluye que al asignar a cada x de A_0 el único y de B tal que $\sigma(x) \cong \sigma(y)$, se obtiene una función $u : A_0 \longrightarrow Y$. Un argumento similar al anterior muestra que u es inyectiva. Además u preserva el orden: si $x, a \in A_0$ y $x \prec a$, sean $u(x) = y$ y $u(a) = b$; esto equivale a $\sigma(x) \cong \sigma(y)$ y $\sigma(a) \cong \sigma(b)$, si fuese $b \prec y$, entonces $\sigma(b) \subset \sigma(y)$; como $\sigma(a) \cong \sigma(b)$ y éste es un segmento inicial de $\sigma(y)$, luego (Prop. 6) $\sigma(y)$ no puede ser semejante a un subconjunto de $\sigma(a)$. en contradicción con el hecho $\sigma(y) \cong \sigma(x)$ y $\sigma(x) \subset \sigma(a)$ ya que $x \prec a$. Se concluye que $y \prec b$ y así u preserva el orden.

De otra parte, A_0 *es una sección de* A: sean $a \in A_0$ y $x \prec a$. Si $b = u(a)$, existe una semejanza $f : \sigma(a) \longrightarrow \sigma(b)$ y por la proposición 1. se sigue que $\sigma(x) \cong \sigma(f(x))$, luego $x \in A_0$.

Análogamente $u(A_0)$ resulta ser una sección de B y como u es inyectiva, $A_0 \cong u(A_0)$. Por la proposición 2,

$$(A_0 = A \vee A_0 = \sigma(a)) \wedge (u(A_0) = B \vee u(A_0) = \sigma(b)),$$

con $a \in A$ y $b \in B$. Distribuyendo,

$$(A_0 = A \wedge u(A_0) = B) \vee (A_0 = A \wedge u(A_0) = \sigma(b)) \\ \vee (A_0 = \sigma(a) \wedge u(A_0) = B) \\ \vee (A_0 = \sigma(a) \wedge u(A_0) = \sigma(b)).$$

La última de las posibilidades no puede darse ya que si sucediese, entonces $\sigma(a) \cong \sigma(b)$ y a sería elemento de A_0 o sea $a \in \sigma(a)$ lo cual es contradictorio.

Tampoco pueden tenerse dos de estas opciones simultáneamente, pues ello implicaría que un conjunto sería igual a uno de sus segmentos iniciales.

Se debe cumplir entonces una única de las tres primeras opciones, con lo cual queda completamente demostrado el teorema 1. □

Ejercicios

1. Dé un ejemplo de un conjunto parcialmente ordenado que tenga una sección que no sea un segmento inicial, ni sea el conjunto completo.

2. Igual que en 1., pero de un conjunto totalmente ordenado.

3. Si $f : A \to B$ es una biyección y B es un conjunto bien ordenado por una relación "$\preceq$", pruebe que la relación "$\preceq$" definida en A mediante $x \preceq y$ si y solo si $f(x) \preceq f(y)$, es un buen orden para A y f se transforma así en una semejanza entre $(A, \preceq)$ y $(B, \preceq)$.

8.2 NÚMEROS ORDINALES

De acuerdo con los resultados de la sección anterior, dos conjuntos bien ordenados semejantes, son desde el punto de vista del orden, prácticamente indistinguibles, de manera que para clasificar conjuntos bien ordenados, bastará asignar a cada uno de ellos un objeto especial, un conjunto bien ordenado prototipo, en forma tal que a dos conjuntos bien ordenados semejantes, corresponda el mismo objeto; éste será su número ordinal, el que caracterizará al tipo de orden del conjunto.

No es posible definir el tipo de orden de un conjunto bien ordenado como la colección de todos los conjuntos bien ordenados semejantes al conjunto dado, ya que dentro de nuestra teoría, dicha colección no puede formarse lícitamente.

Una manera de resolver este problema consiste en proceder de igual forma a como lo hicimos para clasificar conjuntos finitos de acuerdo con su tamaño: asignar a cada conjunto finito un número natural. Los números naturales se definieron de acuerdo a ciertos criterios de economía de símbolos y conceptos; se obtuvieron dotados de una "superestructura", con una riqueza de propiedades mucho mayor de la que teníamos en mente inicialmente; ello se debió a que los naturales así definidos son en realidad números ordinales finitos. Recordemos algunos de ellos:

$$0 = \emptyset; \quad 1 = \{\emptyset\}; \quad 2 = \{\emptyset, \{\emptyset\}\}; \quad 3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \cdots$$

Algunas de sus propiedades notables, son:

1. $(\forall n)(n \notin n)$.

2. Todo natural posee un sucesor inmediato $n^+ = n \cup \{n\}$, el cual por 1., tiene un elemento más que n.

3. Todo elemento de un natural, es subconjunto de dicho natural.

4. La pertenencia es una relación de orden estricto que ordena bien a todo natural (y también a $\mathbb{N}$).

5. Para todo x de n se tiene que $\sigma(x) = x$.

Queremos que los ordinales posean estas mismas propiedades. ¿Cuál podría ser un ordinal que no sea un natural? Según nuestra experiencia, el conjunto $\mathbb{N}$ de todos los naturales sería un firme candidato, ya que para

el orden usual (que es precisamente la pertenencia), es un conjunto bien ordenado y además $\mathbb{N} \notin \mathbb{N}$ ya que $\mathbb{N}$ es infinito y sus elementos son finitos. Cuando se considera a $(\mathbb{N}, \leq)$ como ordinal, se le acostumbra a notar por ω. Para que se cumpla la propiedad 2., deberá existir su sucesor $\omega^+ = \omega \cup \{\omega\} = \{0, 1, 2, 3, ..., \omega\}$. Nuevamente la pertenencia ordena bien a ω^+ y en él ω es su último elemento ya que $(\forall x \neq \omega)(x \in \omega)$; así $\sigma(\omega) = \omega$. La propiedad 2 implica la existencia de $\omega, \omega^+, (\omega^+)^+, ((\omega^+)^+)^+, \cdots$ ¿Existirá un conjunto que contenga a ω y a todos estos sucesores?.

Así como no podemos terminar de definir los naturales de uno en uno y necesitamos del axioma del infinito para producir todos los naturales simultáneamente, aquí necesitamos de un nuevo principio, de un axioma más de la teoría de conjuntos con el cual mostrar la existencia de muchos conjuntos de ordinales. Es el axioma de sustitución (o de reemplazo) que vimos al final del capítulo anterior.

Realmente no es necesario definir "ordinal" como un conjunto que posea todas las propiedades 1 a 5, ya que algunas de ellas se deducen de las otras.

DEFINICIÓN 3. *Un conjunto A se llama* `transitivo` *si todos sus elementos también son subconjuntos de A, es decir, $(\forall x)(x \in A \rightarrow x \subseteq A)$, o sea si cumple la condición 3 anterior.*

En este caso, si $y \in x \wedge x \in A$, entonces $y \in A$, teniéndose una especie de transitividad, la cual da el nombre a la propiedad. Nótese que esto no implica que si x, y, z son elementos de A y $x \in y \wedge y \in z$, entonces $x \in z$.

DEFINICIÓN 4. *Un conjunto α se llama un* `ordinal` *si es transitivo y si la pertenencia es una relación de orden estricto en α que ordena bien a α,*

o sea si cumple las condiciones 3 y 4 anteriores; veamos que también se cumple 1. sin necesidad del axioma de regularidad:

PROPOSICIÓN 7. *Para todo ordinal α se cumple $\alpha \notin \alpha$.*

Demostración. Si se tuviese $\alpha \in \alpha$, entonces α sería un elemento de α y como la pertenencia es un orden estricto en el conjunto α, entonces $\neg(\alpha \in \alpha)$, obteniéndose una contradicción, luego por reducción al absurdo, $\alpha \notin \alpha$. □

PROPOSICIÓN 8. *Todo elemento de un ordinal, es un ordinal.*

Demostración. Sea α un ordinal y sea $\beta \in \alpha$; como α es transitivo, $\beta \subset \alpha$ y la pertenencia restringida a β es un orden estricto para β y lo ordena

bien. Nos resta probar que β es transitivo: sea $y \in \beta$ y $u \in y$; como $\beta \subset \alpha$, entonces $y \in \alpha$ y siendo α transitivo, $y \subset \alpha$ y así también $u \in \alpha$, luego $u, y, \beta \in \alpha$ y siendo la pertenencia una relación transitiva en α (ya que es de orden en α), entonces $u \in \beta$. Se concluye que $y \subseteq \beta$, o sea que β es transitivo. □

PROPOSICIÓN 9. *Si α es un ordinal, $(\forall \beta \in \alpha)(\sigma(\beta) = \beta)$.*

Recordemos que el orden "$\prec$" en α es la pertenencia, luego para todo x, $x \in \sigma(\beta) \leftrightarrow x \prec \beta \leftrightarrow x \in \beta$ y por extensionalidad $\sigma(\beta) = \beta$.

PROPOSICIÓN 10. *Si α es un ordinal, $\alpha^+ = \alpha \cup \{\alpha\}$ también es un ordinal.*

Es sencillo de comprobar que α^+ es transitivo y que también la pertenencia es un buen orden estricto para α^+.

COROLARIO 3. *Para todo ordinal α,* $\sigma(\alpha) = \alpha$.

Como $\alpha \in \alpha^+$, por la proposición 9 se tiene el resultado.

PROPOSICIÓN 11. *Si α, β son ordinales cualesquiera, se cumple exactamente una de las relaciones* $\alpha \in \beta, \quad \alpha = \beta, \quad \beta \in \alpha$.

Demostración. : El que α y β sean transitivos, permite deducir inmediatamente que $\eta = \alpha \cap \beta$ es una sección de α y también de β. Por la proposición 2. η es α o η es un segmento inicial de α y η es β o η es un segmento inicial de β y el corolario de la proposición 5 hace que las disyunciones sean exclusivas:

$$\big[(\eta = \alpha) \underline{\vee} (\eta = \sigma(x), x \in \alpha)\big] \wedge \big[(\eta = \beta) \underline{\vee} (\eta = \sigma(y), y \in \beta)\big].$$

fórmula equivalente a

$$(\eta = \alpha \wedge \eta = \beta) \underline{\vee} (\eta = \alpha \wedge \eta = \sigma(y)) \underline{\vee} (\eta = \sigma(x) \wedge \eta = \beta) \underline{\vee} (\eta = \sigma(x) \wedge \eta = \sigma(y)).$$

equivalente por el corolario de la proposición 10, a

$$(\alpha = \beta) \underline{\vee} (\alpha = y, y \in \beta) \underline{\vee} (\beta = x, x \in \alpha) \underline{\vee} [(\eta = x, x \in \alpha) \wedge (\eta = y, y \in \beta)].$$

o sea $\quad (\alpha = \beta) \underline{\vee} (\alpha \in \beta) \underline{\vee} (\beta \in \alpha) \underline{\vee} (\eta \in \alpha \wedge \eta \in \beta)$.

Pero la última alternativa es imposible ya que de ella se deriva $\eta \in \alpha \cap \beta$, es decir $\eta \in \eta$, en contradicción con la proposición 7, quedando demostrado. □

PROPOSICIÓN 12. *Todo conjunto de ordinales es bien ordenado por la relación de pertenencia .*

Demostración. Es suficiente demostrar que todo conjunto no vacío A de ordinales tiene primer elemento. Sea α cualquier ordinal de A; si $\alpha \cap A = \emptyset$, entonces $\sigma(\alpha) \cap A = \emptyset$ y α es el primer elemento de A ya que todo ordinal menor que α no está en A. Si $\alpha \cap A \neq \emptyset$, como $\alpha \cap A \subseteq \alpha$ y éste es bien ordenado por la pertenencia, $\alpha \cap A$ tiene primer elemento a_0; en particular $a_0 \in \alpha$ o sea $a_0 \prec \alpha$. Si x es cualquier elemento de A, por la tricotomía del orden, $\alpha \prec x$ o $\alpha = x$ o $x \prec \alpha$; en el primer caso por transitividad, $a_0 \prec x$; en el segundo caso $a_0 \prec x = \alpha$; en el tercer caso, $x \in \alpha$, luego $x \in \alpha \cap A$ y así $a_0 \preceq x$. se concluye que a_0 es el primer elemento de A. □

PROPOSICIÓN 13. *Dos ordinales son semejantes si y sólo si son iguales .*

Demostración. Supongamos $\alpha \cong \beta$. Si fuesen distintos, por la tricotomía se tendría $(\alpha \in \beta) \veebar (\beta \in \alpha)$. En el primer caso $\beta \cong \alpha = \sigma(\alpha)$ y así β será semejante a uno de sus segmentos iniciales, en contradicción con el corolario de la proposición 5. Análogamente en el segundo caso se tendría una contradicción: $\alpha \cong \beta = \sigma(\beta)$. En consecuencia, $\alpha = \beta$ quedando demostrado, ya que el recíproco es evidente. □

Ejercicios

1. Pruebe que si α, β son ordinales, entonces $(\alpha \preceq \beta$ si si $\alpha \subseteq \beta)$. Ayuda: es suficiente demostrar que $(\alpha \in \beta \leftrightarrow \alpha \subset \beta)$.

2. Compruebe que α^+ es el mínimo ordinal mayor que α.

3. Pruebe que si un conjunto de ordinales es transitivo, entonces dicho conjunto es un ordinal.

4. Demuestre que la unión de cualquier conjunto de ordinales, es un ordinal, y que es precisamente la mínima cota superior del conjunto. Ayuda: Para probar que es un ordinal, use la proposición 12 y el ejercicio 3. Para la otra parte, recuerde que $\sigma(\alpha) = \alpha$.

5. Demuestre que si A es un conjunto de ordinales tal que

$$(\forall\alpha)(\forall\eta)(\alpha \in A \wedge \eta \prec \alpha \rightarrow \eta \in A),$$

entonces dicho conjunto es un ordinal.

8.3 CONJUNTOS DE ORDINALES

En la sección anterior se vio que uno puede ir formando uno a uno los ordinales sucesores de ω:

$$\omega, \omega^+, \omega^{+^+}, \cdots$$

pero que uno nunca terminaría de construirlos todos, y menos aún podría tener un conjunto al cual pertenecieran todos ellos.

Sin embargo construido $\omega^{(n+1)+}$ (ordinal obtenido de ω al repetir el proceso de formar el sucesor ene más una veces), podemos definir por recurrencia la función:

$$f_n : n^+ = \{0, 1, 2, \cdots, n\} \longrightarrow \{\omega, \omega^+, \cdots \omega^{n+}\} \subseteq \omega^{(n+1)+}.$$

mediante $f_n(0) = \omega$ y para todo k con $0 \leq k < n$, $\quad f_n(k^+) = \big(f_n(k)\big)^+$, es decir, $f_n(0) = \omega$, $f_n(1) = \omega^+$, $f_n(2) = (\omega^+)^+, \cdots$, $f_n(n) = \omega^{n+}$.
Así tenemos realmente una cadena de funciones

$$f_0 \subset f_1 \subset f_2 \subset f_3 \subset \cdots$$

todas ellas finitas (f_n contiene $n+1$ parejas ordenadas). Si en el axioma de reemplazo tomamos $\varphi(x, y)$ como $x \in \mathbb{N} \wedge f_x(x) = y$, ésta es una relación funcional en x, luego dicho axioma implica que para $A = \mathbb{N}$,

$$(\exists B)(\forall y)(y \in B \leftrightarrow (\exists x)(x \in \mathbb{N} \wedge x \in \mathbb{N} \wedge f_n(n) = y)).$$

Dicho conjunto B es precisamente $\{\omega, \omega^+, (\omega^+)^+, \cdots\}$. Si lo unimos con ω mismo, obtenemos el ordinal

$$\{0, 1, 2, \cdots, \omega, \omega^+, \omega^{+^+}, \cdots\},$$

notado comúnmente por $\omega 2$. Realmente consta de dos copias disyuntas de ω, dispuestas la una a continuación de la otra.

Si cuando α es un ordinal notamos a α^{n+} por $\alpha + n$, entonces $\omega 2 = \{0, 1, 2, \cdots, \omega, \omega + 1, \omega + 2, \cdots\}$.

El ordinal siguiente a $\omega 2$ será

$$(\omega 2)^+ = \omega 2 \cup \{\omega 2\} = \{0, 1, 2, \cdots, \omega, \omega + 1, \omega + 2, \cdots, \omega 2\}.$$

Una nueva aplicación del axioma de reemplazo permite obtener el conjunto $\{\omega 2, \omega 2 + 1, \omega 2 + 2, \cdots\}$ y éste unido con $\omega 2$ mismo, produce el ordinal.

$$\omega 3 = \{0, 1, 2, \cdots, \omega, \omega + 1, \omega + 2, \cdots, \omega 2, \omega 2 + 1, \omega 2 + 2, \cdots\}.$$

Después seguirá $\omega 3 + 1, \omega 3 + 2, \omega 3 + 3, \cdots$ y usando otra vez el axioma de reemplazo y la unión con $\omega 3$, se obtiene $\omega 4$. Se va formando así una nueva sucesión de ordinales $\omega, \omega 2, \omega 3, \omega 4, \cdots$.

Una nueva y adecuada aplicación del axioma de sustitución produce el conjunto $\{\omega, \omega 2, \omega 3, \omega 4, \cdots\}$ y su unión produce un ordinal llamado ω^2. A éste le siguen $\omega^2 + 1, \omega^2 + 2, \cdots \omega^2 + \omega, \omega^2 + \omega + 1, \omega^2 + \omega + 2, \cdots, \omega^2 + \omega 2, \omega^2 + \omega 2 + 1, \omega^2 + \omega 2 + 2, \cdots, \omega^2 + \omega 3, \cdots, \omega^2 + \omega 4, \cdots$, y después de todos los de la forma $\omega^2 + \omega n$ aparecen $\omega^2 + \omega^2 = \omega^2 2$, obteniéndose otra sucesión:

$$\omega^2, \omega^2 2, \omega^2 3, \cdots, \omega^3, \cdots, \omega^4, \cdots, \omega^5, \cdots, \omega^\omega, \cdots$$

Al primer ordinal no contable se le acostumbra notar Ω.

Obsérvese que a pesar de que todo ordinal posee sucesor inmediato, existen muchos que no tiene predecesor inmediato: ω, $\omega 2$, $\omega 3, \omega^2$, ω^3, ω^ω, Ω. A aquellos ordinales sin predecesor inmediato se les llama *ordinales límites.*

Dejemos de lado esta interesante dirección y utilicemos el axioma de sustitución para caracterizar los diferentes tipos de conjuntos bien ordenados.

TEOREMA 2. *Para cada conjunto bien ordenado existe un único ordinal con el cual es semejante.*

Demostración.: Debido a que la semejanza es simétrica y transitiva, la unicidad del ordinal se sigue inmediatamente de la proposición 13. Además la proposición 4 implica que la semejanza con un ordinal, si existe, es única, de modo que tan sólo debemos demostrar la existencia del ordinal y de la semejanza.

Sea X un conjunto bien ordenado y definamos como B al conjunto $B = \{x \in X | \sigma(x)$ es semejante a un ordinal$\}$. Éste no es vacío ya que si a es el primer elemento de X, entonces $\sigma(a) = \emptyset$ que es el primer ordinal.

Para cada x de B, el segmento inicial $\sigma(x)$ es semejante a un único ordinal $\beta(x)$ mediante una semejanza $f : \sigma(x) \longrightarrow \beta(x)$. Además si x está en B y $y \prec x$, evidentemente $y \in \sigma(x)$ y por la proposición 1 se tiene, $\sigma(y) \cong \sigma(f(y))$ y como este último es un segmento inicial de un ordinal, también es un ordinal y así $y \in B$ y B es una sección de X.
Si $\varphi(x, y)$ es la condición "$(x \in B) \wedge (y$ es ordinal$) \wedge (\sigma(x) \cong y)$" entonces $\varphi(x, y)$ es funcional en x y por el axioma de reemplazo, para el conjunto B existe un conjunto β tal que

$$\forall y(y \in \beta \leftrightarrow (\exists x)(x \in B \wedge x \in B \wedge y \text{ es ordinal } \wedge \sigma(x) \cong y))$$

Puesto que β es un conjunto de ordinales, es bien ordenado por la relación de pertenencia. Para probar que β es un ordinal es suficiente que (ejercicio 5, sección 2)

$$(\forall\alpha)(\forall\eta)(\eta \prec \alpha \wedge \alpha \in \beta \rightarrow \eta \in \beta).$$

Supongamos $\eta \prec \alpha \wedge \alpha \in \beta$; existe $x \in B$ tal que $\sigma(x) \cong \alpha$ y como el orden entre ordinales es la pertenencia, $\eta \in \alpha$ y siendo $\eta = \sigma(\eta)$, es un segmento inicial de α y por la proposición 1, η es semejante a un segmento inicial de $\sigma(x)$, digamos $\eta \cong \sigma(y)$ con $y \prec x$ y $y \in A$. Entonces $y \in B$ y $\eta \in \beta$, concluyéndose que β es un ordinal. Por esto al asignar a cada x de B el único ordinal semejante a $\sigma(x)$, se obtiene una semejanza de B en β.

La demostración del teorema se completa probando que $X = B$. Si fuese $X \neq B$, como B es una sección, la proposición 2 haría que B fuese un segmento inicial de X, o sea que existiría $x_0 \in X$ tal que $B = \sigma(x_0)$; puesto que $B \cong \beta$, se tendría $\sigma(x_0) \cong \beta$ y x_0 estaría en B, es decir, x_0 estaría en $\sigma(x_0)$, lo cual es una contradicción. □

Como consecuencia de este teorema y de la proposición 13, tenemos:

COROLARIO 4. *Dos conjuntos bien ordenados son semejantes si y sólo si ellos son semejantes al mismo ordinal.*

Se dice en este caso que los dos conjuntos poseen el mismo *tipo de orden*; esto significa que desde el punto de vista de su estructura de orden, los dos conjuntos ordenados son indistinguibles. Los ordinales juegan entonces el papel de clasificadores de los conjuntos bien ordenados.

Las notaciónes introducidas, como $\omega+1, \omega+2, \omega 2, \omega 3, \omega n, \cdots$ sugieren la existencia de operaciones entre números ordinales. Dichas sugerencias son enteramente correctas y para darles precisión, vamos a definirlas.

Sean $(A, \leq)$ y $(B, \preceq)$ conjuntos bien ordenados disyuntos; la suma ordinal de $(A, \leq)$ con $(B, \preceq)$ es el conjunto bien ordenado $(A \cup B, S)$, donde S es la relación (conjunto de parejas ordenadas) obtenida al unir la relación de orden de A con $A \times B$ y con la relación de orden de B, es decir, el orden entre elementos de A es el que ya se tenía ($\leq$), todo elemento de A precede a todo elemento de B ($A \times B$), y el orden entre elementos de B es el que ya se tenia ($\preceq$).

Si $\alpha = ord(A, \leq)$ y $\beta = ord(B, \preceq)$, entonces la suma de los ordinales α y β se define como $\alpha+\beta = ord(A \cup B, S)$ por ejemplo, $\omega+2$ sería el ordinal del conjunto bien ordenado $0 < 1 < 2 < \ldots < a < b$, mientras que $2+\omega$ sería el ordinal del conjunto bien ordenado $a < b < 0 < 1 < 2 < \cdots$ que es el mismo ω. Se concluye que

$$2+\omega = \omega \neq \omega+2.$$

Este ejemplo muestra que la adición de ordinales no es conmutativa; dicho comportamiento un tanto desagradable se debe a que cuando agregamos los dos elementos al comienzo de ω por ejemplo, el resultado es un conjunto bien ordenado semejante al inicial, pero si los agregamos al final de ω, el conjunto bien ordenado obtenido posee en particular último elemento y ya no es semejante a ω.

El concepto de suma ordinal puede extenderse a un número infinito de sumandos: si $(A_i, \preceq_i)_{i \in I}$ es una familia de conjuntos bien ordenados disyuntos dos a dos y el conjunto I también es bien ordenado, la suma ordinal de la familia es el conjunto $(\bigcup_{i \in I} A_i, S)$ ordenado en la forma siguiente: dentro de cada A_i el orden es el que ya se tenía, y si $i < j$, todo elemento de A_i precede a todo elemento de A_j. Si $(\alpha_i)_{i \in I}$ es una familia de ordinales tal que $\alpha_i = ord(A_i, \preceq_i)$ entonces $\sum_{i \in I} \alpha_i$ se define como el ordinal de la suma ordinal de la familia $(A_i, \preceq_i)_{i \in I}$.

¿Cómo se define el *producto ordinal* de dos conjuntos bien ordenados $(A, \leq)$ y $(B, \preceq)$?. Puesto que $A \times B = \bigcup_{b \in B} A \times \{b\}$, el producto puede verse como la unión de una familia $(A_b)_{b \in B}$ de conjuntos bien ordenados disyuntos dos a dos con indices en el conjunto bien ordenado B, luego el producto ordinal puede verse como la suma ordinal $(\bigcup_{b \in B} A \times \{b\})$ de dicha familia, es decir, $(a, b) S (c, b')$ si y solo si $(b < b') \vee (b = b' \wedge a \leq c)$.

Así $A \times B$ resulta bien ordenado por el orden lexicográfico inverso.

Si $\alpha = ord(A, \leq)$ y $\beta = ord(B, \preceq)$, entonces el producto ordinal $\alpha\beta$ se define como $ord(A \times B, S)$. Por ejemplo, $\omega 2$ viene a ser el ordinal de $\omega \times \{0, 1\}$ con el orden lexicográfico inverso, o sea el ordinal de

$$(0,0) < (1,0) < (2,0) < \ldots < (0,1) < (1,1) \prec (2,1) < \ldots$$

conjunto semejante a $0 < 1 < 2 < \ldots < \omega < \omega+1 < \omega+2 < \ldots$ mientras que 2ω es el ordinal de $\{0, 1\} \times \omega$ con el orden lexicográfico inverso, es decir el ordinal de

$$(0,0) < (1,0) < (0,1) < (1,1) < (0,2) < (1,2) < (0,3) < (1,3) < \ldots$$

obtenido al colocar ω copias disyuntas de $0 < 1$, una a continuación de la otra, conjunto este último semejante a ω.

En consecuencia

$$2\omega = \omega \neq \omega 2.$$

y la multiplicación ordinal tampoco es conmutativa.

En general puede verse que $\alpha\beta$ es el ordinal del conjunto bien ordenado obtenido al colocar, la una a continuación de la otra, β copias disyuntas

del cardinal α. En los ejercicios encontrará el lector algunas propiedades adicionales de las operaciones entre ordinales.

Así como al comienzo de la teoría axiomática se probó que no existe un conjunto constituido por todos los conjuntos, también es cierto que

TEOREMA 3. *No existe un conjunto constituido por todos los números ordinales.*

Demostración.: Si existiese tal conjunto, su unión sería también un ordinal (ejercicio 4, sección 2) digamos α, el cual sería el *sup* del conjunto de todos los ordinales, es decir, para todo β ordinal, $\beta \preceq \alpha$; en particular como $\alpha + 1$ es también un ordinal, $\alpha + 1 \preceq \alpha$ lo cual es una contradicción ya que $\alpha \prec \alpha + 1$, quedando demostrado. □

La contradicción a la cual llegamos partiendo de la suposición de que existe el conjunto de todos los ordinales, se llama la paradoja de Burali-Forti, debido a que fue este matemático italiano quien la descubrió y publicó en 1897.

En el capítulo IV se probó el teorema de definición por recurrencia: Dados $a \in X$ y $f : X \to X$, existe una única función $u : \omega \to X$ tal que $u(0) = a$ y para todo $n \in \omega$, $u(n^+) = f(u(n))$. Este resultado puede generalizarse para definir funciones cuyos dominios sean mayores que ω. La diferencia entre ω y cualquier ordinal α estrictamente mayor que ω, está en que en α existen ordinales límites, ordinales que no poseen predecesor inmediato, de manera que además de especificar la imagen de 0 y de decir como se obtiene la imagen de n^+ cuando se conoce la de n, es necesario precisar cómo se calcula la imagen de un ordinal límite. Debido a que éste es un texto introductorio, daremos a continuación y sin demostración, la versión más sencilla del teorema de definición por recurrencia transfinita para un conjunto X bien ordenado. Otra versión muy útil puede estudiarse en [5] o en [6].

TEOREMA 4. (Teorema de definición por recurrencia transfinita) *Sean α un ordinal, $(X, \preceq)$ un conjunto bien ordenado, $a \in X$ y $f : X \to X$. Existe una única función $u : \alpha \to X$ tal que*

i) $u(0) = a$,

ii) $u(\beta^+) = f(u(\beta))$ para todo $\beta \in \alpha$ y

iii) $u(\eta) = sup\ \{u(\beta) | \beta \prec \eta\}$ cuando $\eta \in \alpha$ y η es un ordinal límite.

Su demostración puede verse en [7] y es en buena medida una adaptación de la prueba que dimos en el capítulo IV para el teorema de definición por recurrencia.

Para terminar, vamos a describir una forma de definir los números cardinales como ordinales especiales y mostrar que así no se requiere del axioma de cardinalidad dado en el capítulo VI.

Los ordinales $\omega, \omega + 1, \omega + 2, \omega 2$ y ω^2, son todos numerables, es decir, equipotentes con $\mathbb{N}$. El ordinal ω es el mínimo ordinal equipotente con $\mathbb{N}$, propiedad que hace de él un número cardinal.

En general si A es un conjunto cualquiera, el teorema de la buena ordenación nos garantiza que existe al menos un buen orden "$\preceq$" de A, y por consiguiente $(A, \preceq)$ será semejante a un ordinal α; en particular como la semejanza es una biyección, α será equipotente con A. ¿Existirá el conjunto (no vacío) de todos los ordinales equipotentes con A? La condición para obtenerlo es "α es ordinal y $\alpha \approx A$", pero ¿de qué conjunto debemos separar los elementos que la cumplen?

Nuevamente por el teorema de la buena ordenación, existe un buen orden para $\mathcal{P}(A)$ y con él el conjunto de partes de A es semejante a un ordinal η y en particular $\eta \approx \mathcal{P}(A)$, luego por el teorema de Cantor, si α es un ordinal y $\alpha \approx A$, entonces α es dominado rigurosamente por η, luego para el orden entre ordinales no es posible tener $\eta \preceq \alpha$ (si $\eta \preceq \alpha$, sería η semejante a α o a un segmento inicial de α y por consiguiente $\mathcal{P}(A) \preceq A$, lo cual es contradictorio). Se concluye que $\alpha \prec \eta$ o sea que $\alpha \in \eta$, luego η contiene como elementos a todos los ordinales equipotentes con A, de modo que existe el conjunto

$$\mathcal{O}_A = \{\alpha \in \eta \mid \alpha \text{ es un ordinal} \wedge \alpha \approx A\}.$$

Siendo este conjunto bien ordenado, tiene primer elemento y será precisamente el cardinal de A:

$$Card(A) = \text{ mínimo ordinal equipotente con } A.$$

Claramente si $A \approx B$, entonces $\mathcal{O}_A = \mathcal{O}_B$ y en consecuencia $Card(A) = Card(B)$.

Recíprocamente si $Card(A) = Card(B)$, como $A \approx Card(A)$ y $B \approx Card(B)$, entonces $A \approx B$, obteniéndose así el axioma de cardinalidad.

Esperamos haber dejado al lector con la curiosidad y los conocimientos suficientes para continuar en forma autodidacta el estudio de otros temas más avanzados de la teoría de conjuntos usando textos como [6], [7] u [8].

Ejercicios

1. Pruebe que la suma de ordinales está bien definida. En otras palabras, si $\alpha = ord(A_1, \preceq_1) = ord(A_2, \preceq_2)$ y $\beta = ord(B_1, \preceq_1) = ord(B_2, \preceq_2)$ con $A_1 \cap B_1 = \emptyset$ y $A_2 \cap B_2 = \emptyset$, entonces la suma ordinal de $(A_1, \preceq_1)$ con $(B_1, \preceq_1)$, es semejante a la suma ordinal de $(A_2, \preceq_2)$ con $(B_2, \preceq_2)$.

2. Análogamente, demuestre que la multiplicación de números ordinales está bien definida.

3. Pruebe que para todo ordinal $\alpha \geq \omega$, se cumple que

$$1 + \alpha = \alpha \neq \alpha + 1.$$

4. Demuestre que la suma de ordinales es asociativa y modulativa.

5. Pruebe que un ordinal α es un ordinal límite si y sólo si

$$(\forall \beta)(\beta < \alpha \rightarrow \beta + 1 < \alpha).$$

6. Si α es un ordinal límite, demuestre que

$$\alpha = sup\{\beta \mid \beta < \alpha\}.$$

7. Dé un ejemplo de un ordinal β tal que $1 + \beta = \beta + 1 = \beta^+$.

8. ¿ En qué caso se tendrá para los ordinales α y β que $\alpha + \beta = \beta + \alpha$?

9. Si α, γ son ordinales y $\gamma > 0$, entonces $\alpha + \gamma > \alpha$.

10. Pruebe la propiedad cancelativa a izquierda de la adición: Si

$$\gamma + \alpha = \gamma + \beta$$

entonces

$$\alpha = \beta.$$

11. Dé un contraejemplo para hacer ver que no vale la propiedad cancelativa a derecha de la adición, es decir,

$$\neg(\forall \alpha)(\forall \beta)(\forall \gamma)(\alpha + \gamma = \beta + \gamma \rightarrow \alpha = \beta).$$

12. Pruebe que la multiplicación de ordinales es asociativa y modulativa.

13. Si $(\gamma \neq 0) \wedge (\alpha < \beta)$, entonces $\gamma\alpha < \gamma\beta$.

14. Si $\gamma\alpha < \gamma\beta$, entonces $\alpha < \beta$.

15. Si $(\gamma \neq 0 \wedge \gamma\alpha = \gamma\beta)$, entonces $\alpha = \beta$.

16. Si $\alpha < \beta$, entonces $\alpha\gamma \leq \beta\gamma$.

17. Si $\alpha\gamma < \beta\gamma$, entonces $\alpha < \beta$.

**

Bibliografía

[1] Caicedo, Xavier. *Elementos de lógica y Calculabilidad.* Universidad de los Andes, 1990.

[2] Cantor, George. *Contributions to the founding the Theory of transfinite numbers.* Dover, New York, 1915

[3] Cohen, Paul J. *Set theory and the Continuum hypotesis.* Benjamin, New York, 1966.

[4] Fraenkel, Abraham A. *Set theory and Logic.* Addison-Wesley P.C. Reading, Mass, 1966.

[5] Halmos, Paul R. *Teoría Intuitiva de Conjuntos.* Cecsa, Mexico D.F., 1971.

[6] Krivine Jean Louis. *Axiomatic Set Theory.* Reidel P.C., Dordrecht-Holland, 1971.

[7] Pinter, Charles. *Set Theory.* Addison-Wesley P.C. Reading, Mass, 1971.

[8] Rubin, Jean E. *Set theory for the Mathematician.* Holden-Day, San Francisco, 1967.

[9] Suppes, Patrick. *Teoría Axiomática de Conjuntos.* Norma, Cali, 1968.

[10] Tarski, A. *Introducción a la Lógica y a las Ciencias deductivas.* Espasa-Calpe, Buenos Aires, 1951.

[11] Trejo, César A. *El concepto de Número.* O.E.A., Monografía No. 7, Serie de Matemática. Washington D.C., 1968.

[12] Vasco, Carlos. *Dos operadores iterativos para la teoría de Conjuntos.* Matemática, enseñanza universitaria. No. 6, Agosto \78,págs. 3 a 15.

[13] Vasco, Carlos. *Dos operadores iterativos para la teoría de Conjuntos.* Matemática, enseñanza universitaria. No. 11, Agosto \79,págs. 6 a 11.

Índice de Materias

adición
  de cardinales, 246
  de naturales, 157
alcance de un cuantificador, 27
algebraicos, números, 235
antisimétrica, relación, 105
aplicación, 78
árbol de una fórmula, 10
asimétrica, relación, 119
atómica fórmula, 43
atómica, fórmula, 43
axioma de, del
  fundamentación, 268
  cardinalidad, 244
  conjunto binario, 59
  conjunto de partes, 60
  conjunto vacío, 51
  elección, 219, 221
  extensión, 50
  inducción, 137
  infinito, 134
  la unión, 59
  regularidad, 268
  separación, 53

bien ordenado, conjunto, 122, 279
binaria, operación, 89
buen orden, 122, 279
buena ordenación, teor. de la, 259
Burali-Forti
  paradoja de, 292

cadena
  definición, 118
  descendente infinita, 270, 272
cálculo proposicional, 6, 44
campo de una relación, 69
Cantor, proceso diagonal, 229, 240
Cantor, teorema, 237
Cantor-Bernstein, teorema de, 211
característica, función, 238
cardinal, definición, 293
  finito, 146
cardinales,
  comparabilidad de, 263
  orden entre, 245
  producto de, 247, 265
  suma de, 246, 266
cardinalidad, axioma, 244
cartesiano, producto, 66, 232
clases de equivalencia , 110
clases, teoría de, 50
codominio, 78
comparabilidad de conjuntos bien ordenados, 281
compatible, relación, 113, 117
complejos, números, 204
complemento de un conjunto, 21
completitud de los reales, 200
composición de funciones, 91

condición, definición, 13, 52
conectivos, 6
  y cuantificadores, 27
congruencias en los enteros, 103
conjunción, 4
conjunto
  inductivo, 134
  cociente, 111, 113
  contable, 233
  finito, 146, 217
  infinito, 146, 216
  no contable, 237, 240
  numerable, 227, 232
  referencial, 13
  transitivo, 284
conmutativa, operación, 89
continuación, orden por, 260
contradicción, 11, 36
cortadura, 186
  racional, 186
cota inferior,superior, 120
cuantificador existencial, 14
cuantificadores, 27

De Moivre, teorema de, 206
definición por recurrencia, 151, 154, 155, 293

elección, axioma de, 221
elemento maximal,minimal, 122
enteros,números, 169
equipotencia de conjuntos, 103
estratificación de conjuntos, 268, 270
Eudoxio, 184
existencial, cuantificador, 14
exponenciación de cardinales, 248
  de naturales, 163
extensión
  axioma de, 50
  de una función, 96

familia, 222
Fibonacci, sucesión, 154
filtrante,orden, 124
finito, conjunto, 146
fórmula
  atómica, 43
  bien formada, 6, 41, 44
Frege, definición de cardinal de, 131
función
  característica, 238
  biyectiva, 85
  compuesta, 91
  constante, 80
  definición, 78
  idéntica, 79, 93
  inversa, 95
  inyectiva, 82, 93, 223, 252
  sobreyectiva, 84, 93, 223
fundamentación, axioma de, 268

Hausdorff, principios maximales de, 257
heterológico, paradoja del adjetivo, 38
hipótesis del continuo, 241

idempotencia, 264, 265
idéntica, función, 79, 93
imagen
  directa, 85
  recíproca, 85
implicación, 6
inconsistente, teoría, 36
índices, conjunto de, 222
inducción, principios de, 141, 147
  transfinita, 149
inductivo, conjunto, 134
Inf, 120
infinito,
  conjunto, 146

  según Dedekind, 217
intersección
  de dos conjuntos, 18
  de una colección, 31
inversa
  función, 95
  relación, 73
invertiva, operación, 89
inyección canónica, 79
irreflexividad, 119
isomorfas, estructuras, 277
isomorfismo, 174, 180, 199

Kuratowski, def. de par ordenado de, 64

lema de Zorn, 256
lenguaje
  de primer orden, 41
  objeto, 39
lexicográfico, orden, 126
leyes de De Morgan, 22, 33
libre, variable, 52
ligada, variable, 52
límite, ordinal, 289
lineal, orden, 118

maximal, elemento, 122
metalenguaje, 39
método diagonal de Cantor, 229, 240, 243
minimal, elemento, 122
mínimo, elemento, 119
módulo de una operación, 89
modus ponens, regla, 36
monotonía, propiedad de, 160, 247
multiplicación de cardinales, 167
multiplicación de naturales, 160

negación, tabla de la, 3
números
  algebraicos, 235
  cardinales, 293
  complejos, 204
  enteros, 169
  naturales, 139
  ordinales, 277, 284
  racionales, 177, 231
  reales, 183, 199
  trascendentes, 235

operación binaria, 89
operaciones
  entre conjuntos, 18
  entre enteros, 172
  entre naturales, 157, 160
  sobre colecciones de conjuntos, 31
orden
  buen, 122
  denso, 127
  estricto, 118
  lexicográfico, 126
  lineal, 118
  opuesto, 122
  parcial, 118
  total, 118
ordinal, 277, 283
  de un conjunto bien ordenado, 289
  límite, 289

paradoja
  de Burali-Forti, 292
  de Russell, 38, 55
  del adjetivo heterológico, 38
  del conj. de todos los conjuntos, 37
  del mayor cardinal, 36
  del mentiroso, 38
pareja ordenada, 64
partes,
  conjunto de, 238

partición de un conjunto, 112
paso al cociente de una operación, 114
Peano, axiomas de, 129
pertenencia, relación de, 13
predicados, 42
primer elemento, 119
principios de inducción, 141, 147, 149
  maximales, 257
producto
  cartesiano, 66
  cartesiano de familias, 222
  cartesiano de funciones, 81, 83, 84
proposición, 1, 52

raíces de complejos, 206
racionales, números, 177
rango de un conjunto, 271
recorrido de una relación, 69
recurrencia transfinita, 293
recurrencia, definic. por, 151
referencial, conjunto, 13
regularidad, axioma de, 268
relación, 69, 72, 102
  antisimétrica, 105
  asimétrica, 119
  de buen orden, 122
  de equivalencia, 109
  de orden, 118
  inversa, 73
  orden total, 118
  reflexiva, 104
  simétrica, 104
  transitiva, 106
restricción
  biyectiva maximal, 96, 100, 226
  de una función, 96
retículo, 124
Russell, paradoja de, 37, 55

sección de un conjunto ordenado, 279
segmento inicial, 148, 279
semejanza de conjuntos ordenados, 278
separación, principio, 53
símbolos
  específicos, 42
  lógicos, 42
  proposicionales, 7
subconjunto, 14, 51
sucesión, 153
sucesor de un conjunto, 133
Sup, 120

tablas de verdad, 4, 8
tautologías
  definición, 8
  listado de, 9
teorema de Cantor, 237
  de Cantor-Bernstein, 211
  de comparación de ordinales, 285
    de conj. bien ordenados, 281
  de la buena ordenación, 259
  fundamental, 215, 224
teoría
  de clases, 50
  de tipos, 49
términos, 41
total, orden, 118
transfinita, inducción, 149
transitiva, relación, 106
transitivo, conjunto, 284
trascendente, número, 235
tricotomía del orden entre
  cardinales, 263
  ordinales, 285

último elemento, 120
unión

  axioma de la, 59
  de dos conjuntos, 20
  de funciones, 81, 83, 84, 89
  de una colección, 31
unitario, conjunto, 13, 59
universal, cuantificador, 14

variable
  libre, 52
  ligada, 52
Venn, diagramas de, 18
verdad, tablas de, 4, 8

Zermelo, postulado de, 221
Zermelo-Frankel, teoría de conj. de, 49
Zorn, lema de, 256